

[19] 中华人民共和国国家知识产权局

[51] Int. Cl⁷

H04L 9/08

G06F 17/60



[12] 发明专利申请公开说明书

[21] 申请号 02801849.4

[43] 公开日 2003 年 12 月 24 日

[11] 公开号 CN 1463515A

[22] 申请日 2002.3.27 [21] 申请号 02801849.4

[30] 优先权

[32] 2001. 3. 29 [33] JP [31] 94803/2001

[86] 国际申请 PCT/JP02/02955 2002.3.27

[87] 国际公布 WO02/080446 日 2002.10.10

[85] 进入国家阶段日期 2003.1.24

[71] 申请人 索尼公司

地址 日本东京都

[72] 发明人 石黑隆二

[74] 专利代理机构 中国专利代理(香港)有限公司

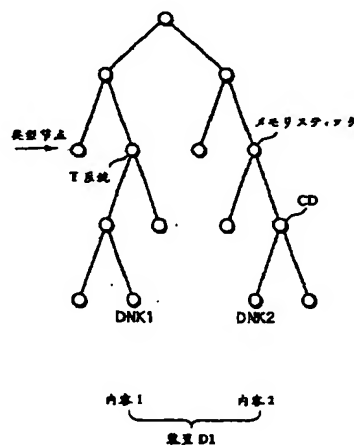
代理人 杨 凯 叶恺东

权利要求书 6 页 说明书 44 页 附图 45 页

[54] 发明名称 信息处理装置

[57] 摘要

提供对内容进行解密的密钥的许可服务器，将密钥管理层次树形结构的叶分配到客户机，生成作为装置节点密钥的节点密钥组，将叶 ID、客户机的秘密密钥等一起向客户机发送。通过以密钥层次结构的中间节点为顶点，以下的节点设定成该顶点节点定义的类型的相关节点，管理类型的顶点节点的制造商、内容提供商等可以独自生成以该节点为顶点的有效密钥块并向顶点节点以下所包含的装置分发，可以在不影响其他类型所包含的装置的情况下更新密钥。



1. 一种信息处理装置, 提供用于内容中包含的有效密钥块(EKB)的解密处理的装置节点密钥, 其特征在于包括:

5 分配单元, 在将内容的提供形态的分类分配到预定层次的第1节点的密钥管理层次树形结构中, 将其他信息处理装置唯一地分配到上述第1节点的下位的叶;

 提供单元, 向上述其他信息处理装置提供从上述分配单元所分配的上述叶到第1节点的路径对应的装置节点密钥。

10 2. 如权利要求1所述的信息处理装置, 其特征在于: 提供上述装置节点密钥的同时, 还提供识别叶的叶识别信息。

 3. 如权利要求2所述的信息处理装置, 其特征在于还包括:

 接收单元, 接收许可请求, 其包含有来自上述其他信息处理装置的上述叶识别信息和识别用以允许利用内容的许可的许可识别信息;

15 发送单元, 发送由附加了上述许可请求中包含的叶识别信息的电子署名构成的许可。

 4. 如权利要求1所述的信息处理装置, 其特征在于: 提供上述装置节点密钥的同时, 还提供上述其他信息处理装置的秘密密钥及公开密钥, 以及自身的公开密钥。

20 5. 一种信息处理方法, 提供用于内容中包含的有效密钥块(EKB)的解密处理的装置节点密钥, 其特征在于包括:

 分配步骤, 在将内容的提供形态的分类分配到预定层次的第1节点的密钥管理层次树形结构中, 将其他信息处理装置唯一地分配到上述第1节点的下位的叶;

25 提供步骤, 向上述其他信息处理装置提供从上述分配步骤的处理所分配的上述叶到上述第1节点的路径对应的装置节点密钥。

 6. 一种记录媒体, 记录计算机可读取的程序, 该程序使信息处

理装置提供用于内容中包含的有效密钥块(EKB)的解密处理的装置节点密钥,其特征在于上述程序包括:

5 分配步骤,在将内容的提供形态的分类分配到预定层次的第1节点的密钥管理层次树形结构中,将其他信息处理装置唯一地分配到上述第1节点的下位的叶;

提供步骤,向上述其他信息处理装置提供从上述分配步骤的处理所分配的上述叶到上述第1节点的路径对应的装置节点密钥。

10 7. 一种程序,使计算机控制信息处理装置,以提供用于内容中包含的有效密钥块(EKB)的解密处理的装置节点密钥,其特征包括:

分配步骤,在将内容的提供形态的分类分配到预定层次的第1节点的密钥管理层次树形结构中,将其他信息处理装置唯一地分配到上述第1节点的下位的叶;

15 提供步骤,向上述其他信息处理装置提供从上述分配步骤的处理所分配的上述叶到上述第1节点的路径对应的装置节点密钥。

8. 一种信息处理装置,提供用以利用内容的许可,其特征包括:

接收单元,接收由上述其他信息处理装置供给的、用以识别分配给其他信息处理装置的密钥管理层次树形结构的叶的叶识别信息;

20 发送单元,在将内容的提供形态的分类分配到预定层次的第1节点的密钥管理层次树形结构中,当上述接收单元接收的上述叶识别信息是上述第1节点的下位的叶的叶识别信息时,发送包含有上述叶识别信息的许可。

25 9. 一种信息处理方法,提供用以利用内容的许可,其特征包括:

接收步骤,接收由上述其他信息处理装置供给的、用以识别分配给其他信息处理装置的密钥管理层次树形结构的叶的叶识别信息;

发送步骤,在将内容的提供形态的分类分配到预定层次的第1节

点的密钥管理层次树形结构中,当由上述接收步骤的处理接收的上述叶识别信息是上述第1节点的下位的叶的叶识别信息时,发送包含有上述叶识别信息的许可。

- 5 10. 一种记录媒体,记录计算机可读取的程序,该程序使信息处理装置提供用以利用内容的许可,其特征在于上述程序包括:

接收步骤,接收由上述其他信息处理装置供给的、用以识别分配给其他信息处理装置的密钥管理层次树形结构的叶的叶识别信息;

- 10 发送步骤,在将内容的提供形态的分类分配到预定层次的第1节点的密钥管理层次树形结构中,当由上述接收步骤的处理接收的上述叶识别信息是上述第1节点的下位的叶的叶识别信息时,发送包含有上述叶识别信息的许可。

11. 一种程序,使计算机控制信息处理装置,以提供用以利用内容的许可,其特征在于包括:

- 15 接收步骤,接收由上述其他信息处理装置供给的、用以识别分配给其他信息处理装置的密钥管理层次树形结构的叶的叶识别信息;

发送步骤,在将内容的提供形态的分类分配到预定层次的第1节点的密钥管理层次树形结构中,当由上述接收步骤的处理接收的上述叶识别信息是上述第1节点的下位的叶的叶识别信息时,发送包含有上述叶识别信息的许可。

- 20 12. 一种提供内容的信息处理装置,其特征在于包括:

接收单元,接收包含有识别内容的内容识别信息的内容请求;

- 25 发送单元,在将内容的提供形态的分类分配到预定层次的第1节点的密钥管理层次树形结构中,发送包含有用与从上述第1节点的下位的叶到上述第1节点的路径对应的装置节点密钥可解密的有效密钥块(EKB)的加密内容。

13. 一种提供内容的信息处理方法,其特征在于包括:

接收步骤,接收包含有识别内容的内容识别信息的内容请求;

发送步骤,在将内容的提供形态的分类分配到预定层次的第1节

点的密钥管理层次树形结构中, 发送包含有用与从上述第 1 节点的下位的叶到上述第 1 节点的路径对应的装置节点密钥可解密的有效密钥块(EKB)的加密内容。

5 14. 一种记录媒体, 记录计算机可读取的程序, 该程序使信息处理装置提供内容, 其特征在于上述程序包括:

接收步骤, 接收包含有识别内容的内容识别信息的内容请求;

发送步骤, 在将内容的提供形态的分类分配到预定层次的第 1 节点的密钥管理层次树形结构中, 发送包含有用与从上述第 1 节点的下位的叶到上述第 1 节点的路径对应的装置节点密钥可解密的有效
10 密钥块(EKB)的加密内容。

15 15. 一种程序, 使计算机控制信息处理装置以提供内容, 其特征在于包括:

接收步骤, 接收包含有识别内容的内容识别信息的内容请求;

发送步骤, 在将内容的提供形态的分类分配到预定层次的第 1 节点的密钥管理层次树形结构中, 发送包含有用与从上述第 1 节点的下位的叶到上述第 1 节点的路径对应的装置节点密钥可解密的有效
15 密钥块(EKB)的加密内容。

16. 一种输出内容的信息处理装置, 其特征在于包括:

存储单元, 存储分配给自身的装置节点密钥, 在将内容的提供形态的分类分配到预定层次的第 1 节点的密钥管理层次树形结构中, 该密钥对应于从上述第 1 节点的下位的叶到上述第 1 节点;
20

内容取得单元, 取得包含有使上述第 1 节点对应于根密钥的有效密钥块(EKB)的加密内容;

解密单元, 通过用上述存储单元存储的装置节点密钥对上述内容取得单元取得的上述加密内容中包含的有效密钥块(EKB)进行的解密处理, 解密上述加密内容;
25

输出单元, 输出由上述解密单元解密的内容。

17. 一种输出内容的信息处理方法, 其特征在于包括:

存储控制步骤，控制分配给自身的装置节点密钥的存储，在将内容的提供形态的分类分配到预定层次的第1节点的密钥管理层次树形结构中，该密钥对应于从上述第1节点的下位的叶到上述第1节点；

- 5 内容取得步骤，取得包含有使上述第1节点对应于根密钥的有效密钥块(EKB)的加密内容；

解密步骤，通过用上述存储控制步骤的处理所存储的装置节点密钥对由上述内容取得步骤的处理所取得的内容中包含的有效密钥块(EKB)进行的解密处理，解密上述加密内容；

- 10 输出步骤，输出由上述解密步骤的处理所解密的内容。

18. 一种记录媒体，记录计算机可读取的程序，该程序使信息处理装置输出内容，其特征在于上述程序包括：

- 15 存储控制步骤，控制分配给自身的装置节点密钥的存储，在将内容的提供形态的分类分配到预定层次的第1节点的密钥管理层次树形结构中，该密钥对应于从上述第1节点的下位的叶到上述第1节点；

内容取得步骤，取得包含有使上述第1节点对应于根密钥的有效密钥块(EKB)的加密内容；

- 20 解密步骤，通过用上述存储控制步骤的处理所存储的装置节点密钥对由上述内容取得步骤的处理所取得的内容中包含的有效密钥块(EKB)进行的解密处理，解密上述加密内容；

输出步骤，输出由上述解密步骤的处理所解密的内容。

19. 一种程序，使计算机控制信息处理装置以输出内容，其特征在于包括：

- 25 存储控制步骤，控制分配给自身的装置节点密钥的存储，在将内容的提供形态的分类分配到预定层次的第1节点的密钥管理层次树形结构中，该密钥对应于从上述第1节点的下位的叶到上述第1节点；

内容取得步骤，取得包含有使上述第1节点对应于根密钥的有效密钥块(EKB)的加密内容；

解密步骤，通过用上述存储控制步骤的处理所存储的装置节点密钥对由上述内容取得步骤的处理所取得的内容中包含的有效密钥块(EKB)进行的解密处理，解密上述加密内容；

输出步骤，输出由上述解密步骤的处理所解密的内容。

信息处理装置

5

技术领域

本发明涉及信息处理装置，具体地说，涉及可以用单个装置管理属于不同类型的内容的信息处理装置。

10

背景技术

最近，随着互联网的普及，提出有通过互联网进行音频和视频等的各种内容的分发的提案并部分地实现在实际应用中。在该情况下，为了保护内容的著作权，对内容规定了各种各样的利用条件，只有满足该利用条件的装置才可以进行利用。

15

但是，以前，在单个装置中对所有的内容以同样的管理形态进行管理。其结果，用单个装置无法逐个对不同服务、利用条件、内容的供给源等的类型进行内容的管理形态的变更，内容的提供者也无法进行柔性管理，在装置的可操作性上存在着问题。

20

发明的公开

本发明针对这样的状况而提出，可以通过单个装置来利用属于不同服务、利用条件、内容的提供源等的类型的多个内容，改进内容提供者、利用者的便利和装置的操作性。

25

本发明的第1信息处理装置，其特征为包括：分配单元，在将内容的提供形态的分类分配到预定层次的第1节点的密钥管理层次树形结构中，将其他信息处理装置唯一地分配到第1节点的下位的叶；提供单元，向其他信息处理装置提供从分配单元所分配的叶到第1节点的路径对应的装置节点密钥。

提供上述装置节点密钥的同时，还可以提供识别叶的叶识别信息。

还可以包括：接收单元，接收许可请求，其包含有来自上述其他信息处理装置的叶识别信息和识别用以允许利用内容的许可的许可识别信息；发送单元，发送由附加了许可请求中包含的叶识别信息的电子署名构成的许可。

提供上述装置节点密钥的同时，还可以提供其他信息处理装置的秘密密钥及公开密钥，以及自身的公开密钥。

本发明的第1信息处理方法，其特征为包括：分配步骤，在将内容的提供形态的分类分配到预定层次的第1节点的密钥管理层次树形结构中，将其他信息处理装置唯一地分配到第1节点的下位的叶；提供步骤，向其他信息处理装置提供从分配步骤的处理所分配的叶到第1节点的路径对应的装置节点密钥。

本发明的第1记录媒体的程序，其特征为包括：分配步骤，在将内容的提供形态的分类分配到预定层次的第1节点的密钥管理层次树形结构中，将其他信息处理装置唯一地分配到第1节点的下位的叶；提供步骤，向其他信息处理装置提供从分配步骤的处理所分配的叶到第1节点的路径对应的装置节点密钥。

本发明的第1程序使计算机实现以下步骤，即：分配步骤，在将内容的提供形态的分类分配到预定层次的第1节点的密钥管理层次树形结构中，将其他信息处理装置唯一地分配到第1节点的下位的叶；提供步骤，向其他信息处理装置提供从分配步骤的处理所分配的叶到第1节点的路径对应的装置节点密钥。

本发明的第2信息处理装置，其特征为包括：接收单元，接收由其他信息处理装置供给的、用以识别分配给其他信息处理装置的密钥管理层次树形结构的叶的叶识别信息；发送单元，在将内容的提供形态的分类分配到预定层次的第1节点的密钥管理层次树形结构中，当接收单元接收的叶识别信息是第1节点的下位的叶的叶识别

信息时，发送包含有叶识别信息的许可。

5 本发明的第2信息处理方法，其特征为包括：接收步骤，接收由其他信息处理装置供给的、用以识别分配给其他信息处理装置的密钥管理层次树形结构的叶的叶识别信息；发送步骤，在将内容的提供形态的分类分配到预定层次的第1节点的密钥管理层次树形结构中，当由接收步骤的处理接收的叶识别信息是第1节点的下位的叶的叶识别信息时，发送包含有叶识别信息的许可。

10 本发明的第2记录媒体的程序，其特征为包括：接收步骤，接收由其他信息处理装置供给的、用以识别分配给其他信息处理装置的密钥管理层次树形结构的叶的叶识别信息；发送步骤，在将内容的提供形态的分类分配到预定层次的第1节点的密钥管理层次树形结构中，当由接收步骤的处理接收的叶识别信息是第1节点的下位的叶的叶识别信息时，发送包含有叶识别信息的许可。

15 本发明的第2程序使计算机实现以下步骤，即：接收步骤，接收由其他信息处理装置供给的、用以识别分配给其他信息处理装置的密钥管理层次树形结构的叶的叶识别信息；发送步骤，在将内容的提供形态的分类分配到预定层次的第1节点的密钥管理层次树形结构中，当由接收步骤的处理接收的叶识别信息是第1节点的下位的叶的叶识别信息时，发送包含有叶识别信息的许可。

20 本发明的第3信息处理装置，其特征为包括：接收单元，接收包含有识别内容的内容识别信息的内容请求；发送单元，在将内容的提供形态的分类分配到预定层次的第1节点的密钥管理层次树形结构中，发送包含有用与从第1节点的下位的叶到第1节点的路径对应的装置节点密钥可解密的有效密钥块(EKB)的加密内容。

25 本发明的第3信息处理方法，其特征为包括：接收步骤，接收包含有识别内容的内容识别信息的内容请求；发送步骤，在将内容的提供形态的分类分配到预定层次的第1节点的密钥管理层次树形结构中，发送包含有用与从第1节点的下位的叶到第1节点的路径对

应的装置节点密钥可解密的有效密钥块(EKB)的加密内容。

5 本发明的第3记录媒体的程序,其特征为包括:接收步骤,接收包含有识别内容的内容识别信息的内容请求;发送步骤,在将内容的提供形态的分类分配到预定层次的第1节点的密钥管理层次树形结构中,发送包含有用与从第1节点的下位的叶到第1节点的路径对应的装置节点密钥可解密的有效密钥块(EKB)的加密内容。

10 本发明的第3程序使计算机实现以下步骤,即:接收步骤,接收包含有识别内容的内容识别信息的内容请求;发送步骤,在将内容的提供形态的分类分配到预定层次的第1节点的密钥管理层次树形结构中,发送包含有用与从第1节点的下位的叶到第1节点的路径对应的装置节点密钥可解密的有效密钥块(EKB)的加密内容。

15 本发明的第4信息处理装置,其特征为包括:存储单元,存储分配给自身的装置节点密钥,在将内容的提供形态的分类分配到预定层次的第1节点的密钥管理层次树形结构中,该密钥对应于从第1节点的下位的叶到第1节点;内容取得单元,取得包含有使第1节点对应于根密钥的有效密钥块(EKB)的加密内容;解密单元,通过用存储单元存储的装置节点密钥对内容取得单元取得的加密内容中包含的有效密钥块(EKB)进行的解密处理,解密加密内容;输出单元,输出由解密单元解密的内容。

20 本发明的第4信息处理方法,其特征为包括:存储控制步骤,控制分配给自身的装置节点密钥的存储,在将内容的提供形态的分类分配到预定层次的第1节点的密钥管理层次树形结构中,该密钥对应于从第1节点的下位的叶到第1节点;内容取得步骤,取得包含有使第1节点对应于根密钥的有效密钥块(EKB)的加密内容;解密步骤,通过用存储控制步骤的处理所存储的装置节点密钥对由内容取得步骤的处理所取得的加密内容中包含的有效密钥块(EKB)进行的解密处理,解密加密内容;输出步骤,输出由解密步骤的处理所解密的内容。

25

本发明的第4记录媒体的程序，其特征为包括：存储控制步骤，控制分配给自身的装置节点密钥的存储，在将内容的提供形态的分类分配到预定层次的第1节点的密钥管理层次树形结构中，该密钥对应于从第1节点的下位的叶到第1节点；内容取得步骤，取得包含有使第1节点对应于根密钥的有效密钥块(EKB)的加密内容；解密步骤，通过用存储控制步骤的处理所存储的装置节点密钥对由内容取得步骤的处理所取得的加密内容中包含的有效密钥块(EKB)进行的解密处理，解密加密内容；输出步骤，输出由解密步骤的处理所解密的内容。

10 本发明的第4程序使计算机实现以下步骤，即：存储控制步骤，控制分配给自身的装置节点密钥的存储，在将内容的提供形态的分类分配到预定层次的第1节点的密钥管理层次树形结构中，该密钥对应于从第1节点的下位的叶到第1节点；内容取得步骤，取得包含有使第1节点对应于根密钥的有效密钥块(EKB)的加密内容；解密步骤，通过用存储控制步骤的处理所存储的装置节点密钥对由内容取得步骤的处理所取得的加密内容中包含的有效密钥块(EKB)进行的解密处理，解密加密内容；输出步骤，输出由解密步骤的处理所解密的内容。

20 本发明的第1信息处理装置、方法及程序中，在将内容的提供形态的分类分配到预定层次的第1节点的密钥管理层次树形结构中，其他信息处理装置被唯一地分配给第1节点的下位的叶，与从该分配的叶到第1节点的路径对应的装置节点密钥提供给其他信息处理装置。

25 本发明的第2信息处理装置、方法及程序中，接收由其他信息处理装置供给的、用以识别分配给其他信息处理装置的密钥管理层次树形结构的叶的叶识别信息；在将内容的提供形态的分类分配到预定层次的第1节点的密钥管理层次树形结构中，当该接收的叶识别信息是第1节点的下位的叶的叶识别信息时，发送包含有叶识别信

息的许可。

本发明的第3信息处理装置、方法及程序中，接收包含有识别内容的
内容识别信息的内容请求；在将内容的提供形态的分类分配到
预定层次的第1节点的密钥管理层次树形结构中，发送包含有用与
5 从第1节点的下位的叶到第1节点的路径对应的装置节点密钥可解
密的有效密钥块(EKB)的加密内容。

本发明的第4信息处理装置、方法及程序中，控制分配给自身的
装置节点密钥的存储，在将内容的提供形态的分类分配到预定层次
的第1节点的密钥管理层次树形结构中，该密钥对应于从第1节点
10 的下位的叶到第1节点；取得包含有使第1节点对应于根密钥的有
效密钥块(EKB)的加密内容；通过用装置节点密钥对所取得的加密内
容中包含的有效密钥块(EKB)进行的解密处理，解密加密内容；输出
所解密的内容。

15 图面的简单说明

图1是表示采用本发明的内容提供系统的构成的方框图。

图2是表示图1的客户机的构成的方框图。

图3是说明图1的客户机的内容的下载处理的流程图。

图4是说明图1的内容服务器的内容提供处理的流程图。

20 图5是表示图4的步骤S26中的格式的示例的图。

图6是说明图1的客户机的内容再现处理的流程图。

图7是说明图6的步骤S43的许可取得处理的详细流程图。

图8是表示许可的结构图。

图9是说明图1的许可服务器的许可提供的处理的流程图。

25 图10是说明图6的步骤S45中的许可更新处理的详细流程图。

图11是说明图1的许可服务器的许可更新处理的流程图。

图12是说明密钥的结构图。

图13是说明类型节点的图。

- 图 14 是表示节点和装置的对应的具体例的图。
- 图 15A 是说明有效密钥块的结构图。
- 图 15B 是说明有效密钥块的结构图。
- 图 16 是说明有效密钥块的利用的图。
- 5 图 17 是表示有效密钥块的格式的示例的图。
- 图 18 是说明有效密钥块的标记的结构图。
- 图 19 是说明采用 DNK 的内容解密处理的图。
- 图 20 是表示有效密钥块的示例的图。
- 图 21 是说明多个内容分配给单个装置的图。
- 10 图 22 是说明许可的类型的图。
- 图 23 是说明登录处理时序图。
- 图 24 是说明客户机的剥离处理的流程图。
- 图 25 是说明水印的结构图。
- 图 26 是表示内容的格式的示例的图。
- 15 图 27 是表示公开密钥证书的示例的图。
- 图 28 是说明内容的分发的图。
- 图 29 是说明客户机的内容的注销处理的流程图。
- 图 30 是说明通过标记追踪有效密钥块的示例的图。
- 图 31 是表示有效密钥块的构成例的图。
- 20 图 32 是说明标志的结构图。
- 图 33 是说明客户机的许可购买处理的流程图。
- 图 34 是说明许可服务器的许可购买处理的流程图。
- 图 35 是表示标志的构成示例的图。
- 图 36 是说明客户机的证书的登录处理的流程图。
- 25 图 37 是说明内容服务器的证书登录处理的流程图。
- 图 38 是表示组的证书的示例的图。
- 图 39 是说明进行分组时的内容服务器的处理的流程图。
- 图 40 是表示内容密钥的加密的示例的图。

图 41 是说明属于组的客户机的处理的流程图。

图 42 是说明对其他客户机进行许可注销的客户机的处理的流程图。

5 图 43 是说明从其他客户机接收许可注销的客户机的处理的流程图。

图 44 是说明接收了许可注销的客户机的再现处理的流程图。

图 45 是说明从其他客户机接受许可的登记的客户机的处理的流程图。

10 图 46 是说明向其他客户机进行许可的登记的客户机的处理的流程图。

图 47 是说明 MAC 的生成的图。

图 48 是说明 ICV 生成密钥的解密处理的流程图。

图 49 是说明 ICV 生成密钥的其他解密处理的图。

图 50A 是说明通过 ICV 进行的许可的拷贝的管理的图。

15 图 50B 是说明通过 ICV 进行的许可的拷贝的管理的图。

图 51 是说明许可的管理的图。

发明的最佳实施例

20 图 1 是表示采用本发明的内容提供系统的结构。互联网 2 中连接有客户机 1-1、1-2 (以下, 不必要区别这些客户机时, 仅称为客户机 1)。该例中虽然只表示了 2 台客户机, 但是互联网 2 中可以连接任意的台数的客户机。

25 另外, 互联网 2 中还连接有向客户机 1 提供内容的内容服务器 3; 向客户机 1 赋予利用内容服务器 3 提供的内容所必要的许可的许可服务器 4; 以及客户机 1 接收许可时, 向该客户机 1 进行收费处理的收费服务器 5。

这些内容服务器 3、许可服务器 4 以及收费服务器 5 也可以任意的台数连接到互联网 2。

图 2 表示客户机 1 的构成。

图 2 中, CPU(Central Processing Unit: 中央处理单元)21 根据 ROM(Read Only Memory: 只读存储器)22 中存储的程序或从存储部 28 加载到 RAM(Random Access Memory)23 的程序, 进行各种的处理。计时器 20 进行计时动作, 将时刻信息供给 CPU21。RAM23 中另外还适当存储有 CPU21 进行各种处理所必要的的数据等。

加密解密部 24 对内容数据进行加密, 并对已加密的内容数据进行解密处理。编解码器部 25, 例如, 采用 ATRAC(Adaptive Transform Acoustic Coding: 自适应变换声编码)3 方式等对内容数据进行编码, 通过输入输出接口 32 提供给与驱动器 30 连接的半导体存储器 44 并记录。或者, 编解码器部 25 通过驱动器 30 从半导体存储器 44 读出编码的数据, 进行解码。

半导体存储器 44, 例如, 由メモリスティック(商标)等构成。

CPU21、ROM22、RAM23、加密解密部 24 以及编解码器部 25 经由总线 31 相互连接。该总线 31 还与输入输出接口 32 连接。

输入输出接口 32 中连接有由键盘、鼠标等构成的输入部 26, 由 CRT、LCD 等构成的显示器, 以及由扬声器等构成的输出部 27, 硬盘等构成的存储部 28, 调制解调器、终端适配器等构成的通信部 29。通信部 29 通过互联网 2 进行通信处理。通信部 29 还与其他客户机之间进行模拟信号或数字信号的通信处理。

根据需要, 输入输出接口 32 还连接驱动器 30, 适当安装磁盘 41、光盘 42、光磁盘 43 或半导体存储器 44 等, 从其中读出的计算机程序根据需要安装在存储部 28。

另外, 虽然省略了图示, 内容服务器 3、许可服务器 4、收费服务器 5 也由具有与图 2 所示客户机 1 基本同样结构的计算机构成。这里, 以下的说明中, 图 2 的结构也作为内容服务器 3、许可服务器 4、收费服务器 5 等的结构被引用。

以下, 参照图 3 的流程图, 说明客户机 1 接收内容服务器 3 提供

的内容的处理。

用户若通过操作输入部 26, 指示接入内容服务器 3, 则在步骤 S1 中, CPU21 控制通信部 29, 使之通过互联网 2 接入内容服务器 3。步骤 S2 中, 用户若操作输入部 26, 指定要接收提供的内容, 则 CPU21 接受该指定信息, 从通信部 29 通过互联网 2 向内容服务器 3 通知指定的内容。参照图 4 的流程图, 如后所述, 由于接收该通知的内容服务器 3 发送来加密的内容数据, 因而在步骤 S3 中, 若 CPU21 经由通信部 29 接收该内容数据, 则在步骤 S4 中将该加密的内容数据供给构成存储部 28 的硬盘并存储。

以下, 参照图 4 的流程图, 说明与客户机 1 的以上处理对应的内容服务器 3 的内容提供处理。另外, 以下说明中, 图 2 的客户机 1 的结构也可作为内容服务器 3 的结构引用。

步骤 S21 中, 内容服务器 3 的 CPU21 处于待机状态, 直到从互联网 2 经由通信部 29 接受了客户机 1 的接入, 判定接受了接入时, 进入步骤 S22, 获取指定客户机 1 发送来的内容的信息。指定该内容的信息是图 3 的步骤 S2 中由客户机 1 通知的信息。

步骤 S23 中, 内容服务器 3 的 CPU21 从存储部 28 存储的内容数据中, 读出步骤 S22 的处理中获取的信息所指定的内容。在步骤 S24 中, CPU21 将从存储部 28 读出的内容数据供给加密解密部 24, 用内容密钥 Kc 进行加密。

由于存储部 28 存储的内容数据通过编解码器部 25 已经进行了 ATRAC3 方式的编码, 因而该编码的内容数据成为加密状态。

另外, 当然, 在存储部 28 中可以以预先加密的状态存储内容数据。该情况下, 可省略步骤 S24 的处理。

以下, 步骤 S25 中, 内容服务器 3 的 CPU21 向构成传送加密内容数据的格式的报头附加解密加密内容所必要的密钥信息(参照图 5, 后述的 EKB(Enabling Key Block)和 $K_{EKB}(Kc)$)和用以识别内容利用所必要的许可的许可 ID。然后, 在步骤 S26 中, 内容服务器 3 的 CPU21

将步骤 S24 的处理中加密的内容和步骤 S25 的处理中附加了密钥和许可 ID 的报头经过格式化后的数据,从通信部 29 通过互联网 2 发送到接入的客户机 1。

图 5 表示象这样从内容服务器 3 向客户机 1 供给内容时的格式的结构。如图所示,该格式由报头(Header)和数据(Data)构成。

报头中配置有内容信息(Content information)、URL(Uniform Resource Locator: 统一资源定位地址)、许可 ID(License ID)、有效密钥块(EKB(Enabling Key Block)),以及用 EKB 生成的密钥 K_{EKBC} 加密的内容密钥 Kc 即数据 $K_{EKBC}(Kc)$ 。另外,后面将参照图 15A 及图 15B 描述 EKB。

内容信息包含有用以识别作为数据被格式化的内容数据的识别信息即内容 ID(CID)以及该内容的编解码方式等的信息。

URL 是取得由许可 ID 规定的许可时接入的地址信息,在图 1 的系统的情况下,具体地说,是接受许可所必要的许可服务器 4 的地址。许可 ID 在利用作为数据被记录的内容时识别必要的许可。

数据由任意个数的加密块(Encryption Block)构成。各加密块由初始向量(IV(Initial Vector))、种子(Seed)、以及内容数据用密钥 Kc 加密后的数据 $EK'c(data)$ 构成。

密钥 Kc 如下式所示,由对内容密钥 Kc 和由随机数所设定的值 Seed 应用哈希函数后运算出的值构成。

$$K'c = \text{Hash}(Kc, \text{Seed})$$

初始向量 IV 和种子 Seed 对各加密块设定成不同的值。

该加密是将内容数据以 8 比特为单位区分后,对每 8 比特进行的。后级的 8 比特的加密以利用前级的 8 比特的加密结果进行的 CBC(Cipher Block Chaining: 密码分组链接)模式执行。

CBC 模式的情况下,对最初的 8 比特的内容数据加密时,由于不存在前级的 8 比特的加密结果,因而对最初的 8 比特的内容数据加密时,将初始向量 IV 作为初始值进行加密。

通过进行该 CBC 模式的加密,即使有一个加密块被解码,也不会影响到其他加密块。

另外,该加密将参照图 47 在后面详细描述。

5 另外,对加密方式不限于此,也可以仅仅用内容密钥 Kc 加密内容数据。

这样,客户机 1 可以免费从内容服务器 3 自由取得内容。从而,可以大量分发内容本身。

但是,各客户机 1 在利用取得的内容时,有必要保持许可。这里参照图 6,说明客户机 1 再现内容时的处理。

10 步骤 S41 中,客户机 1 的 CPU21 取得用户通过操作输入部 26 指示的内容的识别信息(CID)。该识别信息例如由内容的标题和赋予存储的各内容的编号等构成。

15 然后,若内容被指示,则 CPU21 读取与该内容对应的许可 ID(使用该内容所必要的许可 ID)。如图 5 所示,该许可 ID 记述于加密的内容数据的报头。

以下,进入步骤 S42, CPU21 判定是否通过客户机 1 已经取得与在步骤 S41 中读取的许可 ID 对应的许可并存储到存储部 28。另外,在许可未取得的情况下,进入步骤 S43, CPU21 执行许可取得处理。该许可取得处理的详细情况将参照图 7 的流程图在后面描述。

20 在步骤 S42 中,在判定许可已经取得的情况下,或者,在步骤 S43 中,许可取得处理执行的结果为已取得许可的情况下,进入步骤 S44, CPU21 判定取得的许可是否在有效期限内。许可是否在有效期限内是通过比较作为许可内容的规定的期限(参照后述的图 8)和由计时器 20 计时的现在日期和时间进行判断。当判定许可的有效期限为已经到期的情况下,进入步骤 S45,由 CPU21 执行许可更新处理。该许可更新处理的详细情况将参照图 10 的流程图在后面描述。

25 在步骤 S44 中,判定许可还在有效期限内,或者,在步骤 S45 中,许可被更新的情况下,进入步骤 S46, CPU21 从存储部 28

读出加密的内容数据，存储到 RAM23。然后，步骤 S47 中，以配置成图 5 的数据的加密块为单位，CPU21 将 RAM23 中存储的加密块的数据提供给加密解密部 24，用内容密钥 Kc 解密。

5 将参照图 15A 及图 15B 在后面叙述获得内容密钥 Kc 的方法的具体例，利用装置节点密钥 (DNK (Device Node Key)) 可获得 EKB (图 5) 所包含的密钥 K_{EKBC} ，利用该密钥 K_{EKBC} 可从数据 $K_{EKBC}(Kc)$ (图 5) 获得内容密钥 Kc。

10 在步骤 S48 中，CPU21 还将加密解密部 24 解密的内容数据提供给编解码器部 25 进行解码。然后，CPU21 将由编解码器部 25 解码的数据从输入输出接口 32 提供给输出部 27，进行 D/A 变换，并从扬声器输出。

以下，参照图 7 的流程图，详细说明图 6 的步骤 S43 中进行的许可取得处理。

15 客户机 1 通过事先接入许可服务器进行登录处理，取得叶 ID、DNK (Device Node Key)、客户机 1 的秘密密钥·公开密钥对、许可服务器的公开密钥以及包含各公开密钥的证书的服务数据。客户机的登录处理的详细情况将参照图 23 在后面叙述。

20 叶 ID 表示分配给每个客户机的识别信息，DNK 是对与该许可对应的 EKB (有效密钥块) 中包含的加密内容密钥 Kc 进行解密所必要的装置节点密钥 (参照图 12 在后面叙述)。

25 首先，在步骤 S61 中，CPU21 从图 5 所示的报头取得与作为当前处理对象的许可 ID 对应的 URL。如上述，该 URL 还是取得与报头中记述的许可 ID 对应的许可时应接入的地址。这里，在步骤 S62 中，CPU21 接入在步骤 S61 取得的 URL。具体地说，通过通信部 29 经由互联网 2 接入许可服务器 4。此时，许可服务器 4 请求客户机 1 输入指定购买许可 (内容使用所必要的许可) 的许可指定信息以及用户 ID 和密码 (后述的图 9 的步骤 S102)。CPU21 将该请求显示在输出部 27 的显示部。用户根据该显示操作输入部 26，输入许可指定信息、用

户 ID 及密码。另外, 该用户 ID 和密码是客户机 1 的用户经由互联网 2 接入许可服务器 4 后事先取得的。

在步骤 S63、S64 中, CPU21 获取输入部 26 输入的许可指定信息以及用户 ID 和密码。在步骤 S65 中, CPU21 控制通信部 29, 将输入的用户 ID 和密码、许可指定信息、以及包含有服务数据(后述)中包含的叶 ID 的许可请求通过互联网 2 向许可服务器 4 发送。

参照图 9, 如后所述, 许可服务器 4 根据用户 ID 和密码以及许可指定信息发送许可(步骤 S109), 或, 在条件不满足的情况, 不发送许可(步骤 S112)。

步骤 S66 中, CPU21 判定许可服务器 4 是否发送来许可, 发送来许可的情况下, 进入步骤 S67, 将该许可提供给存储部 28 并存储。

步骤 S66 中, 判定许可未发送的情况下, 进入步骤 S68, CPU21 执行错误处理。具体地说, 由于 CPU21 未获得利用内容的许可, 因而禁止内容的再现处理。

这样, 各客户机 1 取得与附加有内容数据的许可 ID 对应的许可, 可开始使用该内容。

另外, 图 7 的许可取得处理可以在各用户取得内容之前预先进行。

如图 8 所示, 向客户机 1 提供的许可包含使用条件、叶 ID 等。

使用条件中包括以下信息: 根据该许可, 可使用内容的使用期限; 根据该许可, 可下载内容的下载期限; 根据该许可, 可进行内容拷贝的次数(允许拷贝次数)、注销次数、最大注销次数; 根据该许可, 可将内容记录到 CD-R 的权利; 可拷贝到 PD(Portable Device: 便携装置)的次数; 将许可转成所有权(购买状态)的权利, 使用记录的义务等。

以下, 参照图 9 的流程图, 说明与图 7 的客户机 1 的许可取得处理对应执行的许可服务器 4 的许可提供处理。另外, 该情况中, 图 2 的客户机 1 的结构也作为许可服务器 4 的结构被引用。

步骤 S101 中, 许可服务器 4 的 CPU21 处于待机状态, 直到接受客户机 1 的接入, 在接受接入时, 进入步骤 S102, 请求接入的客户机 1 发送用户 ID 和密码以及许可指定信息。这样, 当客户机 1 发送来图 7 的步骤 S65 的处理中的用户 ID、密码、叶 ID 以及许可指定信息(许可 ID)时, 许可服务器 4 的 CPU21 通过通信部 29 执行接收和获取处理。

然后, 在步骤 S103 中, 许可服务器 4 的 CPU21 通过通信部 29 接入收费服务器 5, 请求进行与用户 ID 和密码对应的用户的信贷审核处理。收费服务器 5 若通过互联网 2 从许可服务器 4 接受信贷审核处理的请求, 则调查与该用户 ID 和密码对应的用户的过去的支付履历等, 调查该用户过去是否有未支付许可的价格的实绩, 若无这样的实绩, 则发送允许许可赋予的信贷审核结果, 若有未支付的实绩等情况时, 发送不允许许可赋予的信贷审核结果。

在步骤 S104 中, 许可服务器 4 的 CPU21 判定来自收费服务器 5 的信贷审核结果是否为允许许可赋予的信贷审核结果, 若为允许许可的赋予的情况, 则进入步骤 S105, 将与步骤 S102 的处理中获取的许可指定信息对应的许可从存储部 28 存储的许可中取出。存储部 28 存储的许可预先记述了许可 ID、版本、生成日期时间、有效期限等的信息。在步骤 S106 中, CPU21 向该许可附加接收的叶 ID。而且, 步骤 S107 中, CPU21 选择与步骤 S105 选择的许可对应的使用条件。或者, 在步骤 S102 的处理中由用户指定使用条件的情况下, 根据需要将该使用条件附加到预先准备的使用条件上。CPU21 将选择的使用条件附加到许可上。

步骤 S108 中, CPU21 用许可服务器的秘密密钥对许可进行署名, 从而, 生成图 8 所示结构的许可。

以下, 进入步骤 S109, 许可服务器 4 的 CPU21 将该许可(具有图 8 所示结构)从通信部 29 通过互联网 2 向客户机 1 发送。

步骤 S110 中, 许可服务器 4 的 CPU21 使步骤 S109 的处理中的当

前发送的许可(使用条件, 包含叶 ID)与步骤 S102 的处理中获取的用户 ID 和密码对应, 存储到存储部 28。而且, 在步骤 S111 中, CPU21 执行收费处理。具体地说, CPU21 通过通信部 29 请求收费服务器 5 对该用户 ID 和密码对应的用户进行收费处理。收费服务器 5 根据该收费的请求, 对该用户执行收费处理。这样, 对于该收费处理, 若该用户不进行支付, 则以后该用户即使再请求许可的赋予, 也无法接受许可。

即, 该情况下, 由于从收费服务器 5 发送来不允许许可赋予的信贷审核结果, 因而从步骤 S104 进入步骤 S112, CPU21 执行错误处理。具体地说, 许可服务器 4 的 CPU21 控制通信部 29, 向接入的客户机 1 输出无法赋予许可的消息, 并结束处理。

在该情况下, 如上所述, 由于该客户机 1 无法接受许可, 因而无法利用该内容(对加密进行解密)。

图 10 表示图 6 的步骤 S45 中的许可更新处理的详细情况。图 10 的步骤 S131 至步骤 S135 的处理基本上与图 7 的步骤 S61 至步骤 S65 的处理相同。但是, 步骤 S133 中, CPU21 不购买许可, 而是获取更新的许可的许可 ID。然后, 步骤 S135 中, CPU21 向许可服务器 4 发送用户 ID 和密码, 以及更新的许可的许可 ID。

对应步骤 S135 的发送处理, 如后述, 许可服务器 4 提示使用条件(图 11 的步骤 S153)。在步骤 S136 中, 客户机 1 的 CPU21 接收来自许可服务器 4 的使用条件的提示, 将其输出到输出部 27 并显示。用户通过操作输入部 26 来选择该使用条件的中预定的使用条件或新追加预定的使用条件。在步骤 S137 中, CPU21 向许可服务器 4 发送用以购买如上选择的使用条件(更新许可的条件)的申请。如后述, 对应该申请, 许可服务器 4 发送最终的使用条件(图 11 的步骤 S154)。步骤 S138 中, 客户机 1 的 CPU21 从许可服务器 4 取得使用条件, 在步骤 S139 中, 用该使用条件更新存储部 28 中已存储的对应的许可的使用条件。

图 11 表示对应以上的客户机 1 的许可更新处理, 许可服务器 4 执行的许可更新处理。

首先, 在步骤 S151 中, 许可服务器 4 的 CPU21 若接受客户机 1 的接入, 则在步骤 S152 中, 也接收客户机 1 在步骤 S135 中发送的许可指定信息和许可更新请求信息。

步骤 S153 中, CPU21 若接收许可的更新请求, 则从存储部 28 读出与该许可对应的使用条件(更新的使用条件), 发送到客户机 1。

对于该提示, 如上述, 若客户机 1 通过图 10 的步骤 S137 的处理申请购买使用条件, 则在步骤 S154 中, 许可服务器 4 的 CPU21 生成与申请的使用条件对应的数据, 在步骤 S154 中, 向客户机 1 发送。如上述, 客户机 1 利用步骤 S139 的处理中接收的使用条件, 更新已登录的许可的使用条件。

本发明中, 如图 12 所示, 根据广播加密(Broadcast Encryption)方式的原理管理装置和许可的密钥(参照特开 2001-352321 号公报)。密钥采用层次树形结构, 最下级的叶(leaf)对应于各个装置的密钥。在图 12 的示例的情况下, 生成与从编号 0 到编号 15 的 16 个装置或许可对应的密钥。

各密钥规定为与图中的圆符表示的树形结构的各节点对应。该例中, 根密钥 KR 对应于最上级的根节点, 密钥 K0、K1 对应于第 2 级节点, 密钥 K00 至 K11 对应于第 3 级节点, 密钥 K000 至密钥 K111 对应于第 4 级节点。密钥 K0000 至 K1111 分别对应于最下级节点的叶(装置节点)。

由于采用层次结构, 因而密钥 K0010 和密钥 K0011 的上位密钥是 K001, 密钥 K000 和密钥 K001 的上位密钥是 K00。以下同样, 密钥 K00 和密钥 K01 的上位密钥是 K0, 密钥 K0 和密钥 K1 的上位密钥是 KR。

利用内容的密钥由与从最下级的叶到最上级的根节点的单个路径的各节点对应的密钥进行管理。例如, 根据编号 3 的节点(叶 ID)对应的许可来利用内容的密钥, 由包含密钥 K0011、K001、K00、K0、KR

的路径的各密钥进行管理。

本发明的系统中，如图 13 所示，用根据图 12 的原理构成的密钥系统对装置的密钥和许可的密钥进行管理。图 13 的示例中，8+24+32 级节点采用树形结构，类型对应于从根节点到下位的 8 级为止的各节点。这里的类型是指，例如使用メモリスティック等の半导体存储器的机器的类型，或接收数字播放的机器的类型。作为管理许可系统的本系统(称为 T 系统)与该类型节点中的单个节点对应。

即，通过与比该 T 系统节点更下级的层次的 24 级节点对应的密钥来对应许可。该例中，从而，可以规定 2 的 24 次方(约 16 兆)的许可。而且，通过最下侧的 32 级的层次，可以规定 2 的 32 次方(约 4 千兆)的用户(或客户机 1)。从最下级的 32 级节点对应的叶到根节点为止的路径的各节点对应的密钥构成 DNK (Device Node Key)，最下级的叶对应的 ID 作为叶 ID。

各装置和许可的密钥与由 64 (=8+24+32) 级的各节点所构成的路径内的一个对应。例如，加密内容的内容密钥，用构成分配给对应许可的路径的节点所对应的密钥进行加密。上位层次的密钥用最近的下位层次的密钥进行加密，配置在 EKB(参照图 15A 及图 15B 在后面叙述)内。DNK 不配置在 EKB 内，而是记述在服务数据内，提供给用户的客户机 1。客户机 1 利用服务数据中记述的 DNK，对与内容数据一起分发的 EKB(图 15A 及图 15B)内记述的最近的上位层次的密钥进行解密，利用解密获得的密钥，对 EKB 内记述的更上级的层次的密钥进行解密。通过依次进行以上的处理，客户机 1 可以获得属于该路径的所有密钥。

图 14 表示层次树形结构的类型的分类的具体的示例。图 14 中，在层次树形结构的最上级设定根密钥 KR2301，在以下的中间级设定节点密钥 2302，在最下级设定叶密钥 2303。各装置持有各个叶密钥、从叶密钥到根密钥的一系列节点密钥以及根密钥。

从最上级向下第 M 级(图 13 的例中，M=8)的预定节点设定成类型

节点 2304。即第 M 级的各个节点是指定类型的装置设定节点。以第 M 级的单个节点为顶点的 M+1 级以下的节点及叶是该类型所包含的装置相关的节点及叶。

5 例如，在图 14 的第 M 级的一个节点 2305 上设定类型[メモリスティック(商标)]，该节点以下连接的节点、叶设定成包含有使用メモリスティック的各种各样的装置的类型专用节点或叶。即，节点 2305 以下定义成由メモリスティック的类型所定义的装置的关关节点及叶的集合。

10 而且，可以将从 M 级往下数级的下位的级设定成子类型节点 2306。图 14 的例中，在类型[メモリスティック]节点 2305 的 2 级以下的节点中，将[再现专用器]节点 2306 设定为包含有使用メモリスティック的装置的类型子类型节点。而且在子类型节点即再现专用器节点 2306 以下设定再现专用器的类型中包含的带音乐再现机能的电话节点 2307，而且在其下位，还设定带音乐再现机能的电话的类型中包含的[PHS]节点 2308 和[便携电话]节点 2309。

15 而且，类型、子类型不限于装置的种类，可以用例如某制造商、内容提供商、结算机关等独自管理的节点，即处理单位、管辖单位、或提供服务单位等任意的单位（以下通称为实体）进行设定。例如若将单个类型节点设定成游戏机制造商所销售的游戏机 XYZ 专用的顶点节点，则制造商销售的游戏机 XYZ 中可以存储该顶点节点以下的下级节点密钥、叶密钥并进行销售，然后，通过加密内容的分发或各种密钥的分发及更新处理，生成并分发由该顶点节点密钥以下的节点密钥、叶密钥构成的有效密钥块(EKB)，使得只可对顶点节点以下的装置分发可以利用的数据。

20 25 这样，以单个节点为顶点，将以下的节点设定为由该顶点节点定义的类型或子类型的关关节点，通过这样的构成，管理类型级或子类型级的一个顶点节点的制造商、内容提供商等独自生成以该节点为顶点的有效密钥块(EKB)，可以形成向顶点节点以下包含的装置分

发的结构,可以在对不属于该顶点节点的其他类型节点包含的装置完全没有影响的情况下执行密钥更新。

例如,图 12 所示的树形结构中,单个组中包含的四个装置 0、1、2、3 持有作为节点密钥的共用密钥 $K00$ 、 $K0$ 、 KR 。利用该节点密钥共有结构,可以仅仅向装置 0、1、2、3 提供共用内容密钥。例如,若将共同持有的节点密钥 $K00$ 自身设定成内容密钥,则可以不执行新的密钥发送,设定只有装置 0、1、2、3 共用的内容密钥。另外,若用节点密钥 $K00$ 对新的内容密钥 $Kcon$ 加密后的值 $Enc(K00, Kcon)$ 经由网络或存储到记录媒体并分发到装置 0、1、2、3,则只有装置 0、1、2、3 可以用各个装置中持有的共有节点密钥 $K00$ 对密码 $Enc(K00, Kcon)$ 解密而获得内容密钥 $Kcon$ 。另外, $Enc(Ka, Kb)$ 表示用 Ka 加密 Kb 后的数据。

另外,在某时刻 t ,当发现装置 3 所有的密钥 $K0011$ 、 $K001$ 、 $K00$ 、 $K0$ 、 KR 被攻击者(黑客)解析并暴露时,则在这以后,为了对系统(装置 0、1、2、3 的组)中收发的数据进行保密,有必要使装置 3 从系统分离。因而,必须分别用新密钥 $K(t)001$ 、 $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ 更新节点密钥 $K001$ 、 $K00$ 、 $K0$ 、 KR ,并将该更新密钥发送给装置 0、1、2。这里, $K(t)aaa$ 表示密钥 $Kaaa$ 的第 t 代(Generation)的更新密钥。

以下说明更新密钥的分发处理。密钥的更新通过将由图 15A 所示称为有效密钥块(EKB: Enabling Key Block)的块数据构成的表经由网络或存储到记录媒体并提供给装置 0、1、2 来执行。另外,有效密钥块(EKB)由用以将新更新的密钥分发到与构成图 12 所示树形结构的各叶(最下级节点)对应的装置的加密密钥构成。有效密钥块(EKB)也称为密钥更新块(KRB: Key Renewal Block)。

图 15A 所示的有效密钥块(EKB)作为具有这样的数据结构的块数据而构成,即只有需要更新节点密钥的装置才可以进行更新。图 15A 的示例是以向图 12 所示树形结构中的装置 0、1、2 分发第 t 代的更

新节点密钥为目的而形成的块数据。从图 12 可以明显看出, 装置 0、装置 1 需要更新节点密钥 $K(t)00$ 、 $K(t)0$ 、 $K(t)R$, 装置 2 需要更新节点密钥 $K(t)001$ 、 $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ 。

如图 15A 的 EKB 所示, EKB 中包含有多个加密密钥。图 15A 的最下级的加密密钥是 $Enc(K0010, K(t)001)$ 。它是用装置 2 持有的叶密钥 $K0010$ 加密的更新节点密钥 $K(t)001$, 装置 2 用自身持有的叶密钥 $K0010$ 对该加密密钥解密, 可以获得更新节点密钥 $K(t)001$ 。另外, 利用由解密获得的更新节点密钥 $K(t)001$, 图 15A 中从下算起第 2 级的加密密钥 $Enc(K(t)001, K(t)00)$ 变成可解密, 可以获得更新节点密钥 $K(t)00$ 。

以下, 按照顺序, 通过对图 15A 中从上算起第 2 级的加密密钥 $Enc(K(t)00, K(t)0)$ 进行解密, 可获得更新节点密钥 $K(t)0$, 并通过用其对图 15A 中从上算起第 1 级的加密密钥 $Enc(K(t)0, K(t)R)$ 进行解密, 可获得更新根密钥 $K(t)R$ 。

另一方面, 节点密钥 $K000$ 不包含在更新的对象中, 节点 0、1 需要的更新节点密钥是 $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ 。节点 0、1 利用装置节点密钥中包含的节点密钥 $K000$, 通过对图 15A 中从上算起第 3 级的加密密钥 $Enc(K000, K(t)00)$ 进行解密, 取得更新节点密钥 $K(t)00$, 以下, 按照顺序, 通过对图 15A 中从上算起第 2 级的加密密钥 $Enc(K(t)00, K(t)0)$ 进行解密, 获得更新节点密钥 $K(t)0$, 通过对图 15A 中从上算起第 1 级的加密密钥 $Enc(K(t)0, K(t)R)$ 进行解密, 获得更新根密钥 $K(t)R$ 。从而, 装置 0、1、2 可以获得更新的密钥 $K(t)R$ 。

另外, 图 15A 的索引表示图的右侧中作为对加密密钥进行解密的解密密钥使用的节点密钥、叶密钥的绝对地址。

在不必要更新图 12 所示树形结构的上级节点密钥 $K(t)0$ 、 $K(t)R$ 、而只需更新节点密钥 $K00$ 时, 通过利用图 15B 的有效密钥块 (EKB), 可以向装置 0、1、2 分发更新节点密钥 $K(t)00$ 。

图 15B 所示的 EKB 可用于例如在指定的组中分发共有的新内容密

钥的场合。例如，图 12 中虚线所示的组内的装置 0、1、2、3 利用某记录媒体，需要新的共用内容密钥 $K(t)_{con}$ 。此时，将利用装置 0、1、2、3 的共用节点密钥 $K00$ 更新后的 $K(t)00$ 对新的共用更新内容密钥 $K(t)_{con}$ 进行加密后的数据 $Enc(K(t)00, K(t)_{con})$ 与图 15B 所示的 EKB 一起分发。通过该分发，可以分发装置 4 等其他组的机器无法解密的数据。

即，若装置 0、1、2 利用处理 EKB 而获得的密钥 $K(t)00$ 对加密文进行解密，则可获得 t 时刻的内容密钥 $K(t)_{con}$ 。

图 16 中，作为获得 t 时刻的内容密钥 $K(t)_{con}$ 的处理例，表示经由记录媒体接受由 $K(t)00$ 对新的共用内容密钥 $K(t)_{con}$ 加密后的数据 $Enc(K(t)00, K(t)_{con})$ 和图 15B 所示 EKB 的装置 0 的处理。即，该例是将由 EKB 加密的消息数据作为内容密钥 $K(t)_{con}$ 的示例。

如图 16 所示，装置 0 利用记录媒体存储的第 t 代时刻的 EKB 和自身预先存储的 DNK 中包含的节点密钥 $K000$ 进行与上述场合同样的 EKB 处理，生成节点密钥 $K(t)00$ 。而且，装置 0 利用解密的更新节点密钥 $K(t)00$ 对更新内容密钥 $K(t)_{con}$ 进行解密，并用只有自身持有叶密钥 $K0000$ 进行加密并存储，以便在以后使用。

图 17 表示有效密钥块 (EKB) 的格式的示例。版本 601 是表示有效密钥块 (EKB) 的版本的识别符。另外，版本具有识别最新的 EKB 的机能和表示与内容的对应关系的机能。深度表示有效密钥块 (EKB) 的分发目的装置在层次树中的层次数。数据指针 603 是表示有效密钥块 (EKB) 中的数据部 606 的位置的指针，标记指针 604 是表示标记部 607 的位置的指针，署名指针 605 是表示署名 608 的位置的指针。

数据部 606 存储对更新的节点密钥加密后的数据。例如，存储与如图 16 所示的更新节点密钥相关的各加密密钥等。

标记部 607 是表示数据部 606 中存储的加密节点密钥、叶密钥的位置关系的标记。该标记的赋予规则用图 18 进行说明。

图 18 表示发送作为数据的先前图 15A 中说明的有效密钥块 (EKB)

的示例。此时的数据如图 18 的表所示。此时的加密密钥中包含的顶级节点的地址为顶级节点地址。该例中，由于包含有根密钥的更新密钥 $K(t)R$ ，因而顶级节点地址成为 KR 。此时，例如最上级的数据 $Enc(K(t)0, K(t)R)$ 与表示图 18 所示层次树的位置 $P0$ 对应。下一级的数据是 $Enc(K(t)00K(t)0)$ ，在树中与前面的数据的左下位置 $P00$ 对应。从树形结构的预定位置看来，其下存在数据时标记设定为 0，不存在数据时标记设定为 1。标记设定成 {左 (L) 标记, 右 (R) 标记}。由于与图 18 的表的最上级的数据 $Enc(K(t)0, K(t)R)$ 对应的位置 $P0$ 的左下的位置 $P00$ 中存在数据，因而 L 标记=0，而右边不存在数据，因而 R 标记=1。以下，对所有的数据设定标记，构成如图 18 所示的数据列及标记列。

标记设定成表示对应的数据 $Enc(Kxxx, Kyyy)$ 处于树形结构的哪个位置。数据部 606 存储的密钥数据 $Enc(Kxxx, Kyyy)$... 仅仅是单纯的加密密钥的罗列数据，通过上述的标记可判别作为数据存储的加密密钥在树上的位置。若不采用上述的标记，象先前的图 15A 及图 15B 说明的结构一样，采用与加密数据对应的节点索引也可以形成例如

0: $Enc(K(t)0, K(t)R)$

00: $Enc(K(t)00, K(t)0)$

000: $Enc(K((t)000, K(t)00)$

...的数据结构，但是若采用这样的索引的结构，数据变得冗长且数据量增大，不适宜经由网络的分发等。对此，通过采用上述的标记作为表示密钥位置的索引数据，可以以较少的数据量判别密钥位置。

回到图 17，进一步说明 EKB 格式。署名 (Signature) 608 是发行有效密钥块 (EKB) 的密钥管理中心 (许可服务器 4)、内容提供商 (内容服务器 3)、结计算机关 (收费服务器 5) 等执行的电子署名。接受了 EKB 的装置通过署名验证来确认是合法的有效密钥块 (EKB) 发行者发行的有效密钥块 (EKB)。

这样, 根据许可服务器 4 供给的许可利用由内容服务器 3 供给的内容的处理归纳成如图 19 所示。

5 即, 从内容服务器 3 向客户机 1 提供内容的同时, 从许可服务器 4 向客户机 1 提供许可。内容用内容密钥 K_c 进行加密 ($Enc(K_c, Content)$), 内容密钥 K_c 用根密钥 K_R (从 EKB 获得的密钥, 与图 5 中的密钥 K_{EKB} 对应) 进行加密 ($Enc(K_R, K_c)$), 与 EKB 一起附加到加密的内容, 提供给客户机 1。

10 图 19 的例中的 EKB 中, 例如, 如图 20 所示, 包含有用 DNK 可解密的根密钥 $K_R (Enc(DNK, K_R))$ 。从而, 客户机 1 利用服务数据中包含的 DNK, 可以从 EKB 获得根密钥 K_R 。而且, 利用根密钥 K_R , 可以从 $Enc(K_R, K_c)$ 解密出内容密钥 K_c , 利用内容密钥 K_c , 可以从 $Enc(K_c, Content)$ 解密出内容。

这样, 通过个别地向客户机 1 分配 DNK, 根据参照图 12 及图 15A、图 15B 说明的原理, 可以进行各个客户机 1 的撤消 (revoke)。

15 另外, 通过向许可附加叶 ID 并分发, 可在客户机 1 中进行服务数据和许可的对应, 可以防止许可的非法拷贝。

另外, 通过将客户机用的证书和秘密密钥作为服务数据进行分发, 最终用户也可以利用其生成可防止非法拷贝的内容。

后面将参照图 29 的流程图叙述证书和秘密密钥的利用。

20 本发明中, 如参照图 13 所进行的说明, 由于在类型节点中, 管理许可的本发明的内容分发系统和利用各种内容的装置的类型相对应, 因而同一装置可以持有多个 DNK。其结果, 可以用单个装置管理不同的类型的内容。

25 图 21 表示该关系。即, 在装置 D1 中, 根据内容分发系统分配 DNK1, 记录利用内容 1 的许可及服务数据。同样, 在该装置 D1 中, 例如, 可以分配 DNK2, 并在メモリスティック中记录从 CD 剥离的内容 2。该情况下, 装置 D1 可同时处理由称为内容 1 和内容 2 的不同系统 (内容分发系统和装置管理系统) 分发的内容。在分配新 DNK 的

情况下，删除已经分配的 DNK，而只有一个 DNK 与装置对应的情况下则无法进行删除。

5 另外，图 13 中，例如，通过向下侧的 32 层次的每个三角形分配图 22 所示的许可类型 1 和许可类型 2，可利用子类型将同一类型内分类成内容的种类、等级、销售店、分发服务、内容的出处、提供方法等的小集合来进行管理。

10 图 22 的例中，例如，许可类型 1 属于爵士乐的种类，许可类型 2 属于摇滚乐的种类。许可类型 1 中，与许可 ID 为 1 的内容 1 和内容 2 对应，分别分发给用户 1 至用户 3。许可类型 2 包含许可 ID2 的内容 3、内容 4 及内容 5，分别提供给用户 1 和用户 3。

这样，本发明中，可对每个类型进行独立的密钥管理。

另外，可以实现这样的系统，即 DNK 不预先嵌入机器和媒体，在进行登录处理时，通过由许可服务器 4 下载到各机器和媒体，用户可以取得密钥。

15 参照图 23 说明该情况下客户机 1 的登录处理。

步骤 S161 中，客户机 1 的 CPU21 控制通信部 29，向许可服务器 4 发送服务数据请求。在步骤 S165 中，若许可服务器 4 的 CPU21 经由通信部 29 接收输入的服务数据请求，则在步骤 S166 中，经由通信部 29 向客户机 1 发送用户信息请求。

20 在步骤 S162 中，客户机 1 的 CPU21 若经由通信部 29 接收用户信息请求，则控制输出部 27，在显示器等中显示促使用户信息的输入的消息。若用户通过操作键盘等从输入部 26 输入用户本人的个人信息和结算信息等的用户信息，则在步骤 S163 中，客户机 1 的 CPU21 经由通信部 29 向许可服务器 4 发送输入的用户信息。

25 在步骤 S167 中，许可服务器 4 的 CPU21 若经由通信部 29 接收用户信息，则在步骤 S168 中，分配到该许可服务器 4 的类型节点以下的叶中，将未分配的叶分配给客户机 1，生成分配到从该叶到分配给许可服务器 4 的类型节点为止的路径上的节点的节点密钥组，作

为装置节点密钥。将生成的装置节点密钥、分配给客户机 1 的叶的叶 ID、客户机 1 的秘密密钥、客户机 1 的秘密密钥公开密钥对、许可服务器的公开密钥以及各公开密钥的证书汇总，生成服务数据，在步骤 S169 中，经由通信部 29 向客户机发送生成的服务数据，同时，控制驱动器 30，使用户信息与叶 ID 对应地记录在硬盘等的记录媒体上。

在步骤 S164 中，客户机 1 的 CPU21 若经由通信部 29 接收服务数据，则控制加密解密部 24，对接收的服务数据加密，控制驱动器 30，记录在硬盘等的记录媒体上。

这样，许可服务器 4 登录客户机 1 及该用户，客户机 1 可以接收包含有用以利用期望的内容分发服务所必要的装置节点密钥的服务数据。

内容在作成后，无论采用哪种使用方法，都期望可以与该使用方法无关地用于所有用途中。例如，即使在不同内容分发服务或不同域的使用状况的情况下，也期望可以利用同一内容。本发明中为了上述目的，如上所述，从作为认证局的许可服务器 4 向各用户(客户机 1)分发秘密密钥和与之对应的公开密钥的证书(certificates)。各用户利用该秘密密钥，生成署名(Signature)并附加到内容，可以保证内容的完整性(integrity)且防止内容的篡改。

参照图 24 的流程图说明该情况的处理的示例。图 24 的处理说明用户将来自 CD 的再现数据存储到存储部 28 的剥离处理。

首先，在步骤 S171 中，客户机 1 的 CPU21 获取经由通信部 29 输入的 CD 的再现数据，作为记录数据。在步骤 S172 中，CPU21 判定步骤 S171 的处理中获得的记录数据是否包含有水印。该水印由 3 比特的拷贝管理信息(CCI)和 1 比特的触发信号(Trigger)构成，嵌入内容的数据中。CPU21 在检出水印的情况下，进入步骤 S173，执行抽出该水印的处理。水印不存在的情况下，跳过步骤 S173 的处理。

以下，在步骤 S174 中，CPU21 生成对应内容而记录的报头数据。

该报头数据由表示用以获得内容 ID、许可 ID、许可的接入点的 URL、包含水印的拷贝管理信息(CCI)以及触发信号(Trigger)构成。

以下,进入步骤 S175,CPU21 用自身的秘密密钥生成基于步骤 S174 的处理中生成的报头数据的数字署名。该秘密密钥是从许可服务器 4 取得的(图 7 的步骤 S67)。

步骤 S176 中,CPU21 控制加密解密部 24,用内容密钥对内容加密。内容密钥用随机数等生成。

以下,步骤 S177 中,CPU21 根据文件格式,将数据记录到例如由小型盘等构成的光磁盘 43。

另外,记录媒体为小型盘时,在步骤 S176 中,CPU21 将内容供给编解码器部 25,例如,用 ATRAC3 方式对内容编码。然后,编码的数据用加密解密部 24 进一步加密。

图 25 是象这样记录到记录媒体的内容的状态的模式图。从加密的内容(E(At3))抽出的水印(WM)记录在内容之外(报头)。

图 26 表示内容记录到记录媒体时的文件格式的更详细结构。该例中,除了记录有内容 ID(CID)、许可 ID(LID)、URL 及包含水印(WM)的报头,还记录有 EKB、用根密钥 KR 加密内容密钥 Kc 后的数据(Enc(KR, Kc))、证书(Cert)、基于报头生成的数字署名(Sig(Header))、用内容密钥 Kc 加密内容后的数据(Enc(Kc, Content)),中间数据(Meta Data)及标志(Mark)。

水印虽然嵌入内容的内部,但是如图 25 和图 26 所示,也可不在内容的内部而配置在报头内,从而可以迅速且简单地检出水印嵌入内容的信息。从而,可以迅速判定该内容是否可以拷贝。

另外,中间数据表示封套、照片、歌词等的的数据。标志将参照图 32 在后面叙述。

图 27 表示作为证书的公开密钥证书的示例。公开密钥证书通常是公开密钥加密方式中的认证局(CA: Certificate Authority)发行的证书,由认证局向用户向认证局提出的自己的 ID 和公开密钥等附

加有效期限等信息以及认证局的数字署名而生成。本发明中，由于许可服务器 4 (或内容服务器 3) 发行证书和秘密密钥以及公开密钥，用户通过向许可服务器 4 提供用户 ID、密码等进行登录处理，可以获得该公开密钥证书。

5 图 27 中的公开密钥证书包含以下消息：证书的版本编号、许可服务器 4 分配给证书的利用者(用户)的证书的序列号、数字署名采用的算法及参数、认证局(许可服务器 4)的名称、证书的有效期限、证书利用者的 ID(节点 ID 或叶 ID)以及证书利用者的公开密钥。而且，该消息中附加有作为认证局的许可服务器 4 生成的数字署名。
10 该数字署名是根据对消息应用哈希函数而生成的哈希值，利用许可服务器 4 的秘密密钥生成的数据。

 节点 ID 或叶 ID，例如图 12 的示例的情况下，当为装置 0 时为「0000」，当为装置 1 时为「0001」，当为装置 15 时为「1111」。根据这样的 ID，可以识别该装置(实体)是位于树结构的哪个位置(叶
15 或节点)的实体。

 这样，通过将利用内容所必要的许可与内容分离地进行分发，可以自由地进行内容的分发。通过任意的的方法或通路获得的内容都可进行一次元的处理。

 另外，不用说，通过构成图 26 所示的文件格式可以经由互联网
20 分发该格式的内容，即使在提供给 SDMI(Secure Digital Music Initiative: 安全数字音乐自发)机器的情况下，也可以管理内容的著作权。

 而且，例如，如图 28 所示，不论内容是通过记录媒体提供还是通过互联网 2 提供，通过同样的处理，都可以在作为 SDMI(Secure
25 Digital Music Initiative: 安全数字音乐自发)机器的预定的 PD(Portable Device: 便携装置)等中注销。

 以下，参照图 29 的流程图，说明客户机 1 对其他客户机(例如，PD)进行内容注销时的处理。

首先, 在步骤 S191 中, CPU21 判定内容中是否附加了数字署名。当判定附加了数字署名时, 进入步骤 S192, CPU21 抽出证书, 用认证局(许可服务器 4)的公开密钥执行验证处理, 即, 客户机 1 从许可服务器 4 获得与许可服务器 4 的秘密密钥对应的公开密钥, 用该公开密钥对公开密钥证书中附加的数字署名进行解密。如参照图 27 所进行的说明, 数字署名根据认证局(许可服务器 4)的秘密密钥而生成, 可以用许可服务器 4 的公开密钥进行解密。而且, CPU21 对证书的所有消息应用哈希函数来运算哈希值。然后, CPU21 比较运算出的哈希值和对数字署名解密获得的哈希值, 若两者一致, 则判定消息未被篡改。若两者不一致, 则该证书被篡改。

在步骤 S193 中, CPU21 判定证书是否被篡改, 判定未篡改时, 进入步骤 S194, 用 EKB 执行验证证书的处理。该验证处理是根据证书中包含的叶 ID(图 27), 通过调查是否可以追踪 EKB 来进行的。参照图 30 和图 31 对该验证进行说明。

现在, 如图 30 所示, 例如, 令持有叶密钥 K1001 的装置为被撤消的装置。此时, 具有如图 31 所示的数据(加密密钥)和标记的 EKB 分发到各装置(叶)。由于撤消了图 30 中的装置「1001」, 该 EKB 成为更新密钥 KR、K1、K10、K100 的 EKB。

被撤消装置「1001」以外的所有叶可以取得更新的根密钥 $K(t)R$ 。即, 由于节点密钥 K0 的下位连接的叶在装置内保持有未更新的节点密钥 K0, 因而可通过用密钥 K0 对加密密钥 $Enc(K0, K(t)R)$ 解密来获得更新根密钥 $K(t)R$ 。

另外, 节点 11 以下的叶利用未更新的节点密钥 K11, 通过用节点密钥 K11 对 $Enc(K11, K(t)1)$ 解密, 可以获得更新节点密钥 $K(t)1$ 。而且, 通过用节点密钥 $K(t)1$ 对 $Enc(K(t)1, K(t)R)$ 解密, 可以获得更新根密钥 $K(t)R$ 。节点密钥 K101 的下位叶同样也可以获得更新根密钥 $K(t)R$ 。

而且, 持有未撤消的叶密钥 K1000 的装置「1000」用自己的叶密

钥 K_{1000} 对 $\text{Enc}(K_{1000}, K(t)_{100})$ 解密, 可以获得节点密钥 $K(t)_{100}$, 用其进一步对上位节点密钥依次进行解密, 可以获得更新根密钥 $K(t)_R$.

5 相对地, 被撤消的装置「1001」由于无法通过 EKB 处理获得自身叶的上位节点的更新节点密钥 $K(t)_{100}$, 因而无法获得更新根密钥 $K(t)_R$.

许可服务器 4 向未撤消的合法装置(客户机 1)分发并存储具有图 31 所示数据和标记的 EKB.

10 各客户机利用该标记可进行 EKB 追踪处理。该 EKB 追踪处理是判定是否可以从上位的根密钥追踪密钥分发树的处理。

例如, 图 30 的叶「1001」的 ID(叶 ID)即「1001」可以看作「1」「0」「0」「1」的 4 个比特, 判定通过从最上位比特开始依次到下位比特, 是否可以追踪树。该判定中, 若比特为 1 则进入右侧, 若为 0 则进入左侧。

15 由于 ID「1001」的最上位比特是 1, 因而从图 30 的根密钥 K_R 进入右侧。EKB 的首先的标记(编号 0 的标记)是 0: {0, 0}, 可判定两个分支都具有数据。该情况下, 由于可以进入右侧, 因而可以追踪到节点密钥 K_1 。

20 以下, 进入节点密钥 K_1 的下位节点。由于 ID「1001」的第 2 比特为 0, 进入左侧。编号 1 的标记表示左侧节点密钥 K_0 的下位的数据的有无, 编号 2 的标记表示节点密钥 K_1 的下位的数据的有无。该标记如图 31 所示为 2: {0, 0}, 表示两个分支都具有数据。从而, 进入左侧可以追踪到节点密钥 K_{10} 。

25 而且, ID「1001」的第 3 比特为 0, 进入左侧。此时, 表示 K_{10} 的下位的数据的有无的标记(编号 3 的标记)为 3: {0, 0}, 判定两个分支都具有数据。从而进入左侧可以追踪到节点密钥 K_{100} 。

而且, ID「1001」的最下位比特为 1, 进入右侧。编号 4 的标记与节点密钥 K_{11} 对应, 编号 5 的标记表示 K_{100} 的下位的数据的代码。

该标记为 5: {0, 1}。从而, 右侧不存在数据。其结果, 无法追踪到节点「1001」, 判定 ID「1001」的装置是无法通过 EKB 获得更新根密钥的装置即被撤消装置。

5 相对地, 例如, 持有叶密钥 K1000 的装置 ID 为「1000」, 与上述情况同样, 若根据 EKB 内的标记进行 EKB 追踪处理, 则可以追踪到节点「1000」。从而, ID「1000」的装置被判定为合法的装置。

回到图 29, CPU21 根据步骤 S194 的验证处理, 在步骤 S195 判定证书是否撤消, 当证书未撤消时, 进入步骤 S196, 执行用证书中包含的公开密钥验证数字署名的处理。

10 即, 如图 27 所示, 证书中包含有证书利用者(内容生成者)的公开密钥, 利用该公开密钥验证图 26 所示的署名(Sig(Header))。即, 通过比较利用该公开密钥对数字署名 Sig(Header)解密而获得的数据(哈希值)和对图 26 所示 Header 应用哈希函数运算后的哈希值, 若两者一致, 则可确认 Header 未被篡改。相对地, 若两者不一致, 则
15 Header 被篡改。

步骤 S197 中, CPU21 判定 Header 是否被篡改, 若未被篡改, 则进入步骤 S198 验证水印。在步骤 S199 中, CPU21 判定水印的验证结果是否可以注销。若可以注销, 则进入步骤 S200, CPU21 执行注销。即, 对注销目的地的客户机 1 转发内容并拷贝。

20 在步骤 S191 中判定不存在数字署名时, 在步骤 S193 中判定证书被篡改时, 在步骤 S195 中判定用 EKB 不可验证证书时, 在步骤 S197 中判定数字署名的验证结果表明报头被篡改时, 或, 在步骤 S199 中判定水印中记述了禁止注销时, 进入步骤 S201, 执行错误处理。即, 该情况下注销被禁止。

25 这样, 从许可服务器 4 向用户分发证书和秘密密钥, 在内容生成时附加数字署名, 可以保证内容的作成者的完整性。从而, 可以防止内容的非法流通。

而且, 通过在内容生成时检出水印, 在数字署名上附加该信息,

可防止水印信息的篡改，保证内容的完整性。

其结果，一旦生成内容，则不论以哪种形态分发，都可以保证原来的内容的完整性。

而且，由于内容不具有使用条件，使用条件附加在许可上，因而
5 通过变更许可内的使用条件，可以一起变更与之相关的内容的使用条件。

以下说明标志的利用方法。本发明中，如上所述，使用条件附加到许可而不是内容上。但是，使用状况会随内容的不同而异。本发明中，如图 26 所示，标志附加到内容上。

10 由于许可和内容是一对多的关系，只在许可的使用条件上述内容的各个使用状况变得困难。这样，通过将使用状况附加到内容上，在用许可进行管理的同时也可以管理各个内容。

该标志中，例如图 32 所示，记述有用户的 ID (叶 ID)、所有权旗标、使用开始时刻及拷贝次数等。

15 而且，标志中附加有根据叶 ID、所有权旗标、使用开始时刻及拷贝次数等的消息生成的数字署名。

在直接购买可在预定的期间使用的内容的许可时 (变更成永久使用期间的情况) 附加所有权旗标。使用开始时刻记述于在预定的期间内开始内容的使用的情况。例如，在下载内容的时期被限制的情况下，
20 在该期限内进行下载时，在其中记述实际下载内容的日期时间。从而，证明是期间内进行的有效的使用。

拷贝次数中记述了作为履历 (日志) 的迄今为止的该内容的拷贝次数。

以下，参照图 33 的流程图，说明用户购买了许可的情况下，向
25 内容附加标志的标志附加处理的示例。

首先，在步骤 S221 中，CPU21 根据来自输入部 26 的用户的指令，通过互联网 2 接入许可服务器 4。

在步骤 S222 中，CPU21 经由输入部 26 获取来自用户的输入，对

应该输入，向许可服务器 4 请求购买许可。

对应该请求，参照图 34 的流程图，如后所述，许可服务器 4 提示购买许可所必要的价格(图 34 的步骤 S242)。步骤 S223 中，客户机 1 的 CPU21 若从许可服务器 4 接受价格的提示，则将其输出到输出部 27 并显示。

用户根据该显示判断是否接受提示的价格，根据该判断结果从输入部 26 输入该判断结果。

在步骤 S224 中，CPU21 根据输入部 26 的输入判定用户是否接受提示的价格，判定接受的情况下，进入步骤 S225，执行向许可服务器 4 通知已接受的处理。

若接收该接受通知，则许可服务器 4 发送来表示价格的购买的信息，即记述了所有权旗标的标志(图 34 的步骤 S244)。在步骤 S226 中，客户机 1 的 CPU21 若接收来自许可服务器 4 的标志，则在步骤 S227 中执行将接收的标志嵌入内容的处理。即，从而，作为与购买的许可对应的内容的标志，图 32 所示的所有权旗标记述的标志与内容对应地进行记录。另外，此时由于消息已被更新，CPU21 也更新数字署名(图 26)并记录到记录媒体。

在步骤 S224 中，当判定未接受从许可服务器 4 提示的价格时，进入步骤 S228，CPU21 向许可服务器 4 通知未接受提示的价格。

对应这样的客户机 1 的处理，许可服务器 4 执行图 34 的流程图所示的处理。

即，首先，在步骤 S241 中，若从客户机 1 发送来许可购买的请求(图 33 的步骤 S222)，则许可服务器 4 的 CPU21 接受该请求，在步骤 S242 中，从存储部 28 读出作为对象的许可的购买所必要的价格，发送给客户机 1。

如上所述，对于这样提示的价格，从客户机 1 发送来是否接受提示的价格的通知。

在步骤 S243 中，许可服务器 4 的 CPU21 判定是否从客户机 1 接

收了接受通知，在判定接收了接受通知时，进入步骤 S244，生成包含有表示作为对象的许可的购买的消息的标志，利用自身的秘密密钥附上数字署名，向客户机 1 发送。如上所述，这样发送的标志记录到客户机 1 的存储部 28 中的对应的内容中(图 33 的步骤 S227)。

5 在步骤 S243 中，当判定未从客户机 1 接收接受通知时，跳过步骤 S244 的处理。即，在该情况下，由于最终未进行许可的购买处理，因而不发送标志。

图 35 表示步骤 S244 中从许可服务器 4 向客户机 1 发送的标志的构成示例。该例中，通过该用户的叶 ID、所有权旗标(Own)以及，基
10 于许可服务器 4 的秘密密钥 S 用叶 ID 和所有权旗标生成的数字署名 Sigs (LeafID, Own)来构成标志。

另外，由于该标志只是对指定的用户的指定的内容有效，在拷贝作为对象的内容后，该拷贝的内容附带的标志成为无效。

这样，即使是内容和许可分离，使用条件与许可对应的情况下，
15 也可实现与各个内容的使用状况对应的服务。

以下说明分组。分组是指适当地集中多个机器和媒体，在一个集合内可以进行内容的自由收发。通常，该分组在个人所有的机器和媒体中进行。以前，该分组对每个组设定一样的组密钥，但是通过使分组化的多个机器和媒体与同一许可对应，可容易地进行分组。

20 另外，通过预先登录各机器，也可以进行分组。以下说明该情况的分组。

该情况下，用户必须预先向服务器登录作为分组对象的机器的证书。参照图 36 和图 37 的流程图说明该证书的登录处理。

首先，参照图 36 的流程图说明客户机(作为分组对象的机器)的
25 证书的登录处理。在步骤 S261 中，客户机 1 的 CPU21 生成作为分组对象的机器的自身的证书。该证书包含自身的公开密钥。

以下，进入步骤 S262，CPU21 根据用户的输入部 26 的输入，接入内容服务器 3，在步骤 S263 中，执行将步骤 S261 的处理中生成的

证书发送到内容服务器 3 的处理。

另外，也可以直接使用从许可服务器 4 接收的证书。

以上的处理对作为分组对象的所有机器进行。

5 以下，参照图 37 的流程图，说明与图 36 的客户机 1 的证书的登录处理对应地进行的内容服务器 3 的证书的登录处理。

首先，在步骤 S271 中，内容服务器 3 的 CPU21 若接收从客户机 1 发送来的证书，则在步骤 S272 中将该证书登录到存储部 28。

10 以上的处理对作为组对象的每个机器进行。其结果，例如图 38 所示，对于每个组，构成该组的装置的证书登录到内容服务器 3 的存储部 28 中。

图 38 所示的示例中，证书 C11 至 C14 作为组 1 的证书登录。这些证书 C11 至 C14 中包含有对应的公开密钥 K_{P11} 至 K_{P14} 。

同样，证书 C21 至 C23 作为组 2 的证书登录，它们包含对应的公开密钥 K_{P21} 至 K_{P23} 。

15 该证书登录到构成以上组的各机器的状态下，若用户向该组所包含的机器请求提供内容，则内容服务器 3 执行图 39 的流程图所示的处理。

首先，在步骤 S281 中，内容服务器 3 的 CPU21 执行存储部 28 存储的证书中、属于该组的证书的验证处理。

20 如参照图 30 和图 31 所进行的说明，该验证处理根据各机器的证书中包含的叶 ID，利用标记追踪 EKB。EKB 也从许可服务器 4 分发到内容服务器 3。通过该验证处理，可排除被撤消的证书。

25 在步骤 S282 中，内容服务器 3 的 CPU21 选择在步骤 S281 的验证处理的结果中有效的证书。然后，在步骤 S283 中，CPU21 用步骤 S282 的处理中选择的各机器的证书的各公开密钥对内容密钥加密。步骤 S284 中，CPU21 将步骤 S283 的处理中加密的内容密钥和内容一起发送到作为对象的组的各机器。

图 38 所示组 1 中，例如，若撤消证书 C14，则可以通过步骤 S283

的处理生成例如图 40 所示的加密数据。

即, 图 40 的示例中, 内容密钥 K_c 用证书 C11 的公开密钥 K_{p11} 、证书 C12 的公开密钥 K_{p12} 或证书 C13 的公开密钥 K_{p13} 进行加密。

5 对应内容服务器 3 的图 39 所示的处理, 接收内容的提供的各组的机器(客户机)执行图 41 的流程图所示的处理。

首先, 在步骤 S291 中, 客户机 1 的 CPU21 接收内容服务器 3 在图 39 的步骤 S284 的处理中发送来的内容和内容密钥。内容预先用内容密钥 K_c 加密, 如上所述, 内容密钥用各机器保持的公开密钥进行加密(图 40)。

10 在步骤 S292 中, CPU21 用自身的秘密密钥进行解密并取得在步骤 S291 的处理中接收的自身地址的内容密钥。然后, 用取得的内容密钥进行内容的解密处理。

例如, 与图 40 的示例所示的证书 C11 对应的机器, 利用与公开密钥 K_{p11} 对应的自身的秘密密钥对加密的内容密钥 K_c 进行解密, 取得内容密钥 K_c 。然后, 用内容密钥 K_c 对内容进一步解密。

同样的处理也对与证书 C12、C13 对应的机器执行。由于被撤消的证书 C14 的机器没有将用自身的公开密钥加密的内容密钥 K_c 附带在内容中发送来, 因而无法对内容密钥 K_c 解密, 从而, 无法用内容密钥 K_c 对内容解密。

20 以上, 对内容密钥(即内容)进行了分组, 但是也可以对许可密钥(许可)进行分组。

这样, 可以不用特别的组密钥和后述的 ICV(Integrity Check Value: 完整性校验值)进行分组。该分组适用于小规模的一组。

25 本发明中, 许可也可以进行注销或登记、移动、拷贝。但是, 这些处理根据 SDMI 所定的规则进行。

以下, 参照图 42 和图 43 的流程图, 说明这样的客户机的许可的注销处理。

首先, 参照图 42 的流程图说明对其他客户机注销许可的客户机

的处理。首先在步骤 S301 中，客户机 1 的 CPU21 读出注销对象的许可的注销次数 N1。由于嵌入图 8 所示的使用条件中，因而该注销次数可以从该使用条件读取。

5 以下，在步骤 S302 中，CPU21 仍然从许可的使用条件读出注销对象的许可的最大注销次数 N2。

然后，在步骤 S303 中，CPU21 比较步骤 S301 的处理中读出的注销次数 N1 和步骤 S302 的处理中读出的最大注销次数 N2，判定注销次数 N1 是否小于最大注销次数 N2。

10 判定注销次数 N1 小于最大注销次数 N2 时，进入步骤 S304，CPU21 从对方各个装置取得对方装置(注销目的地的客户机)的叶密钥，将该叶密钥与当前注销对象的许可 ID 对应地存储在存储部 28 的注销清单中。

15 以下，在步骤 S305 中，CPU21 对步骤 S301 的处理中读出的许可的注销次数 N1 的值加一。在步骤 S306 中，CPU21 根据许可的消息运算 ICV。该 ICV 将参照图 47 至图 51 在后面描述。利用 ICV 可以防止许可的篡改。

20 以下，在步骤 S307 中，CPU21 用自身的公开密钥对注销对象的许可和步骤 S306 的处理中运算的 ICV 进行加密，与 EKB 及证书一起输出并拷贝到对方的装置。而且，在步骤 S308 中，CPU21 将步骤 S306 的处理中运算的 ICV 与对方装置的叶密钥和许可 ID 对应地存储到存储部 28 的注销清单中。

25 步骤 S303 中，当判定注销次数 N1 不小于最大注销次数 N2(例如相等)时，由于已经进行了允许次数的注销，因而无法再执行注销。进入步骤 S309，CPU21 执行错误处理。即，该情况下不执行注销处理。

以下，参照图 43 的流程图，用图 42 的注销处理说明接受许可的注销的客户机的处理。

首先，在步骤 S321 中，向对方装置(注销许可的客户机 1)发送

自身的叶密钥。在步骤 S304 中，该叶密钥由对方的客户机与许可 ID 对应地进行存储。

以下，在步骤 S322 中，从对方的客户机 1 发送来加密的许可和 ICV 以及 EKB 和证书时，CPU21 进行接收。即，该许可、ICV、EKB 及证书是图 42 的步骤 S307 的处理中从对方的装置发送来的。

在步骤 S323 中，CPU21 将步骤 S322 的处理中接收的许可、ICV、EKB 及证书存储到存储部 28。

如上所述，接受许可的注销的客户机 1 在使用接受了注销的该许可再现预定的内容时，执行图 44 的流程图所示的处理。

即，首先在步骤 S341 中，客户机 1 的 CPU21 运算由用户经由输入部 26 指定再现的内容的 ICV。然后，在步骤 S342 中，CPU21 根据证书中包含的公开密钥对存储部 28 存储的加密 ICV 进行解密。

以下，在步骤 S343 中，CPU21 通过步骤 S341 的处理判定当前运算的 ICV 与步骤 S342 的处理读出并解密的 ICV 是否一致。两者一致时，则许可未被篡改。然后进入步骤 S344，CPU21 执行再现对应的内容的处理。

相对地，步骤 S343 中，判定两个 ICV 不一致时，许可有可能已被篡改。因而进入步骤 S345，CPU21 执行错误处理。即，此时，用该许可无法再现内容。

以下，如上所述，参照图 45 的流程图说明客户机接受先前从其他客户机注销的许可的登记的处理。

首先，在步骤 S361 中，CPU21 取得对方装置(归还(登记)许可的客户机 1)的叶密钥和登记对象的许可 ID。以下，在步骤 S362 中，CPU21 判定步骤 S361 中取得的登记对象的许可是否自身向对方装置注销的许可。该判定根据图 42 的步骤 S308 的处理中存储的 ICV、叶密钥及许可 ID 进行。即，判定步骤 S361 取得的叶密钥、许可 ID 及 ICV 是否存储在注销清单中，若存储在其中，则判定是自身注销的许可。

许可是自身注销的许可时，在步骤 S363 中，CPU21 请求删除对

方的装置的许可、EKB 及证书。如后述, 根据该请求, 对方的装置执行许可、EKB 及证书的删除(图 46 的步骤 S383)。

在步骤 S364 中, 由于先前注销的许可再次登记, 因而 CPU21 使该许可的注销次数 N1 减一。

5 步骤 S365 中, CPU21 判定是否正在向对方的装置注销其他许可, 不存在另外正在注销的其他许可时, 进入步骤 S366, CPU21 删除以对方的装置作为登记对象机器的注销清单中的存储内容。相对地, 在步骤 S365 中, 判定存在向对方的装置注销其他许可时, 由于可能接受其他许可的登记, 因而跳过步骤 S366 的处理。

10 步骤 S362 中, 作为登记对象的许可判定为自身不是向对方装置注销的许可时, CPU21 进入步骤 S367, 执行错误处理。即, 该情况下, 由于不是自身管辖的许可, 因而不执行登记处理。

用户非法拷贝许可时, 由于存储的 ICV 的值和根据步骤 S361 的处理中取得的许可运算的 ICV 的值不同, 无法进行登记。

15 图 46 表示与图 45 的流程图所示执行许可的登记处理的客户机对应的登记自身具有的许可的客户机的处理。

步骤 S381 中, 客户机 1 的 CPU21 向对方的装置(执行图 45 的流程图所示的处理的客户机 1)发送叶密钥和登记对象的许可 ID。如上所述, 对方的装置在步骤 S361 中取得该叶密钥和许可 ID, 在步骤 S362 中根据该叶密钥和许可 ID 执行登记对象的许可的认证处理。

20 步骤 S382 中, 客户机 1 的 CPU21 判定是否有来自对方装置的许可的删除请求。即, 许可是合法登记对象的许可的情况下, 如上所述, 对方的装置请求在步骤 S363 的处理中删除许可、EKB 及证书。若接收到该请求, 则进入步骤 S383, CPU21 删除许可、EKB 及证书。

25 即, 从而, 该客户机 1 变成以后无法使用该许可的状态, 通过图 45 的步骤 S364 的处理令注销次数 N1 减一, 从而登记结束。

步骤 S382 中, 判定对方的装置未请求删除许可时, 进入步骤 S384, 执行错误处理。即, 该情况下, 由于 ICV 的值不同等的理由,

无法进行登记。

以上，说明了登记和注销，对许可的拷贝或移动也是一样。

以下，说明生成用以防止篡改许可(内容也一样)的许可的完整性校验值(ICV)，与许可对应，通过 ICV 的计算判定许可篡改的有无的处理结构。

许可的完整性校验值(ICV)是通过对许可应用哈希函数，由 $ICV = \text{hash}(K_{icv}, L1, L2, \dots)$ 来计算。 K_{icv} 是 ICV 生成密钥。 $L1$ 、 $L2$ 是许可的信息，使用许可的重要信息的信息认证代码(MAC: Message authentication Code)。

采用 DES 加密处理结构的 MAC 值生成例如图 47 所示。如图 47 的结构所示，作为对象的消息分割成 8 比特单位，(以下，令分割的消息为 $M1$ 、 $M2$ 、...、 M_N)，首先，由运算部 24-1A 对初始值(IV)和 $M1$ 执行异或(令其结果为 $I1$)。接着，将 $I1$ 输入 DES 加密部 24-1B，用密钥(以下为 $K1$)加密(令输出为 $E1$)。然后，由运算部 24-2A 对 $E1$ 及 $M2$ 执行异或，该输出 12 输入 DES 加密部 24-2B，用密钥 $K1$ 加密(输出 $E2$)。以下，反复上述操作，对所有的消息执行加密处理。最后从 DES 加密部 24-NB 输出的 E_N 成为消息认证代码(MAC(Message Authentication Code))。

通过向这样的许可的 MAC 值和 ICV 生成密钥应用哈希函数来生成许可的完整性校验值(ICV)。例如，比较许可生成时生成的 ICV 和基于新的许可生成的 ICV，若可获得同一的 ICV，则可保证许可无篡改，若 ICV 不同，则判定有篡改。

以下，说明通过上述的有效密钥块来发送许可的完整性校验值(ICV)生成密钥即 K_{icv} 的结构。即，以由 EKB 加密的消息数据作为许可的完整性校验值(ICV)生成密钥的示例。

图 48 及图 49 表示，向多个装置发送共用许可时，通过有效密钥块(EKB)分发用以验证这些许可篡改有无的完整性校验值生成密钥 K_{icv} 的结构例。图 48 表示分发装置 0、1、2、3 可解密的校验值生

成密钥 K_{icv} 的示例, 图 49 表示撤消(排除)了装置 0、1、2、3 中的装置 3 后, 分发只有装置 0、1、2 可解密的校验值生成密钥 K_{icv} 的示例。

图 48 的示例中, 由更新节点密钥 $K(t)00$ 对校验值生成密钥 K_{icv} 加密, 生成并分发数据 $Enc(K(t)00, K_{icv})$, 同时, 生成并分发用装置 0、1、2、3 中各自持有的节点密钥、叶密钥可对更新的节点密钥 $K(t)00$ 解密的有效密钥块(EKB)。如图 48 的右侧所示, 各个装置首先通过处理(解密)EKB, 取得更新的节点密钥 $K(t)00$, 然后, 利用取得的节点密钥 $K(t)00$ 对加密的校验值生成密钥 $Enc(K(t)00, K_{icv})$ 解密, 可获得校验值生成密钥 K_{icv} 。

其他装置 4、5、6、7...即使接收同一有效密钥块(EKB), 也无法用自身持有的节点密钥、叶密钥来处理 EKB 并取得更新的节点密钥 $K(t)00$, 因而, 可以安全地只向合法装置发送校验值生成密钥。

另一方面, 图 49 的示例表示, 图 12 的虚线框围成的组中, 装置 3 因为泄漏密钥而被撤消(排除)后, 生成并分发只有其他组的成员即装置 0、1、2 可解密的有效密钥块(EKB)。分发图 49 所示的有效密钥块(EKB)和用节点密钥($K(t)00$)对校验值生成密钥(K_{icv})加密后的数据 $Enc(K(t)00, K_{icv})$ 。

图 49 的右侧表示解密次序。首先, 装置 0、1、2 用自身持有的叶密钥或节点密钥对接受的有效密钥块进行解密处理, 取得更新节点密钥($K(t)00$)。然后, 通过 $K(t)00$ 的解密来取得校验值生成密钥 K_{icv} 。

图 12 所示的其他组的装置 4、5、6...即使接收同样的数据(EKB), 也无法用自身持有的叶密钥、节点密钥来取得更新节点密钥($K(t)00$)。同样, 在被撤消的装置 3 中, 也无法用自身持有的叶密钥、节点密钥来取得更新节点密钥($K(t)00$), 只有具有合法权利的装置可以对校验值生成密钥解密并利用。

这样, 如果利用 EKB 进行校验值生成密钥的分发, 可使得数据量

减少, 并且安全地分发只有合法权利者可解密的校验值生成密钥。

采用这样的许可的完整性校验值(ICV), 可以排除 EKB 和加密许可的非法拷贝。例如, 如图 50A 所示, 假设许可 L1 和许可 L2 以及可取得它们的许可密钥的有效密钥块(EKB)一起存储于媒体 1, 并将其直接拷贝到媒体 2 的情况。可以拷贝 EKB 和加密许可, 在可解密 EKB 的装置中利用它们。

图 50B 所示的例中采用这样的结构, 即, 与各媒体中合法存储的许可对应, 存储有完整性校验值(ICV(L1, L2))。另外, (ICV(L1, L2))表示许可 L1 和许可 L2 中用哈希函数计算的许可的完整性校验值 $ICV = \text{hash}(K_{icv}, L1, L2)$ 。图 50B 的结构中, 媒体 1 中合法存储有许可 1 和许可 2, 存储有根据许可 L1 和许可 L2 生成的完整性校验值(ICV(L1, L2))。另外, 媒体 2 中合法存储有许可 1, 存储有根据许可 L1 生成的完整性校验值(ICV(L1))。

该结构中, 若媒体 1 中存储的 {EKB, 许可 2} 拷贝到媒体 2, 则在媒体 2 中, 若新生成许可校验值, 则可生成与媒体 2 中存储的 $K_{icv}(L1)$ 不同的 ICV(L1, L2), 可以明白通过许可的窜改或非法拷贝执行了新的许可的存储。在再现媒体的装置中, 在再现步骤之前的步骤中执行 ICV 校验, 判别生成 ICV 和存储 ICV 的一致性, 不一致时, 不执行再现, 因而可以防止非法拷贝的许可的再现。

另外, 为了进一步提高安全性, 也可采用根据包含有重写计数值的数据来生成许可的完整性校验值(ICV)的结构。即通过 $ICV = \text{hash}(K_{icv}, \text{counter}+1, L1, L2, \dots)$ 进行计算的结构。这里, 计数值(counter+1)设定成每次改写 ICV 就加一的值。另外, 计数值必须存储在安全的存储器中。

而且, 在许可的完整性校验值(ICV)不可以与许可存储于同一媒体的结构中, 许可的完整性校验值(ICV)也可以在别的媒体上进行存储。

例如, 在读取专用媒体和通常的 MO 等未采取防拷贝对策的媒体

5 中存储许可时,若在同一媒体中存储完整性校验值(ICV),则非法用户有可能改写ICV,无法保证ICV的安全性。这种情况下,通过采用在主机上的安全媒体中存储ICV,在许可的拷贝控制(例如登记/注销、移动)中使用ICV的结构,可以进行ICV的安全管理及许可的篡改校验。

10 该构成例如图51所示。图51中的示例中,读取专用媒体和通常的MO等未采取防拷贝对策的媒体2201中存储许可1至许可3,这些许可相关的完整性校验值(ICV)存储到不允许用户自由接入的主机上的安全媒体2202中,可以防止用户非法改写完整性校验值(ICV)。采用这样的结构,例如,安装有媒体2201的装置执行媒体2201的再现时,通过在主机即PC、服务器中执行ICV的校验来判定可否进行再现,可以防止非法拷贝许可或篡改许可的再现。

15 适用本发明的客户机除了所谓个人计算机以外,还可以是PDA(Personal Digital Assistants: 个人数字助理)、便携电话机、游戏终端机等。

通过软件执行一系列处理时,构成该软件的程序可从网络 and 记录媒体安装到嵌入专用硬件的计算机,或通过安装各种程序可执行各种机能的通用个人计算机等中。

20 如图2所示,该记录媒体不仅可以与装置本体分离,由记录有用以向用户提供程序所分发的程序的磁盘41(包含软盘)、光盘42(包含CDROM(Compact Disk Read Only Memory: 只读光盘存储器),DVD(Digital Versatile Disk: 数字化视频光盘))、光磁盘43(包含MD(Mini Disk: 小型磁盘))或半导体存储器44等组成的分组媒体构成,也可以由以预先内置于装置本体的状态提供给用户的、记录有程序的ROM22和存储部28中包含的硬盘等构成。

25 另外,本说明书中,记述记录媒体中记录的程序的步骤当然包括以记载的顺序按照时间系列进行的处理,也包含不一定按照时间系列而并行执行或个别执行的处理。

另外，执行与保密关联的处理的程序为了防止该处理被解析，最好对该程序自身进行加密。例如，对于进行加密处理等的处理，可以将该程序构成为抗篡改模块。

5 另外，用以指定允许利用内容的许可的记载于内容的报头中的信息，也可以不是唯一地识别许可的许可 ID。上述的实施例中，许可 ID 是指定利用内容所必要的许可的信息，某一许可是指定允许利用的内容的信息，是根据来自客户机 1 的许可请求要求的识别许可的信息。内容中可记载与内容本身相关的各种属性信息的清单，许可中可记载该许可允许利用的内容的条件式。该情况下，内容所包含的
10 的属性信息是指定允许利用该内容的许可的信息，许可所包含的条件式是指定该许可允许利用的内容的信息，许可 ID 成为唯一地识别许可的信息。这种情况下，多个许可可以与一个内容对应，可以弹性地进行许可的发行。

15 另外，内容数据不限于音乐数据。例如，内容也可以是画像数据、动画数据、文本数据、动画数据、软件程序或它们的组合。

另外，本说明书中，系统表示由多个装置构成的装置全体。

产业上的利用可能性

20 如上所述，根据本发明的第 1 信息处理装置，可以对各个提供形态管理密钥。

根据本发明的第 2 信息处理装置，可以对各个提供形态管理密钥。

根据本发明的第 3 信息处理装置，可以对应多个内容的提供形态。

25 根据本发明的第 4 信息处理装置，可以保持多个不同装置节点密钥。

图1

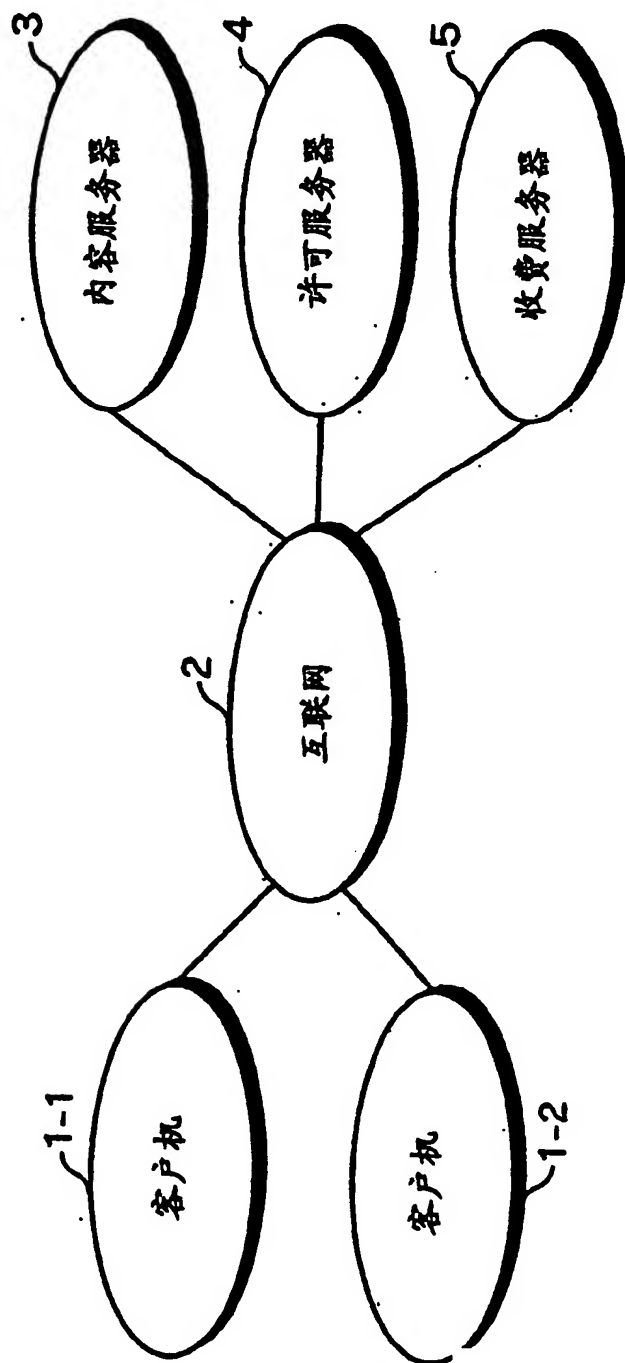


图 2

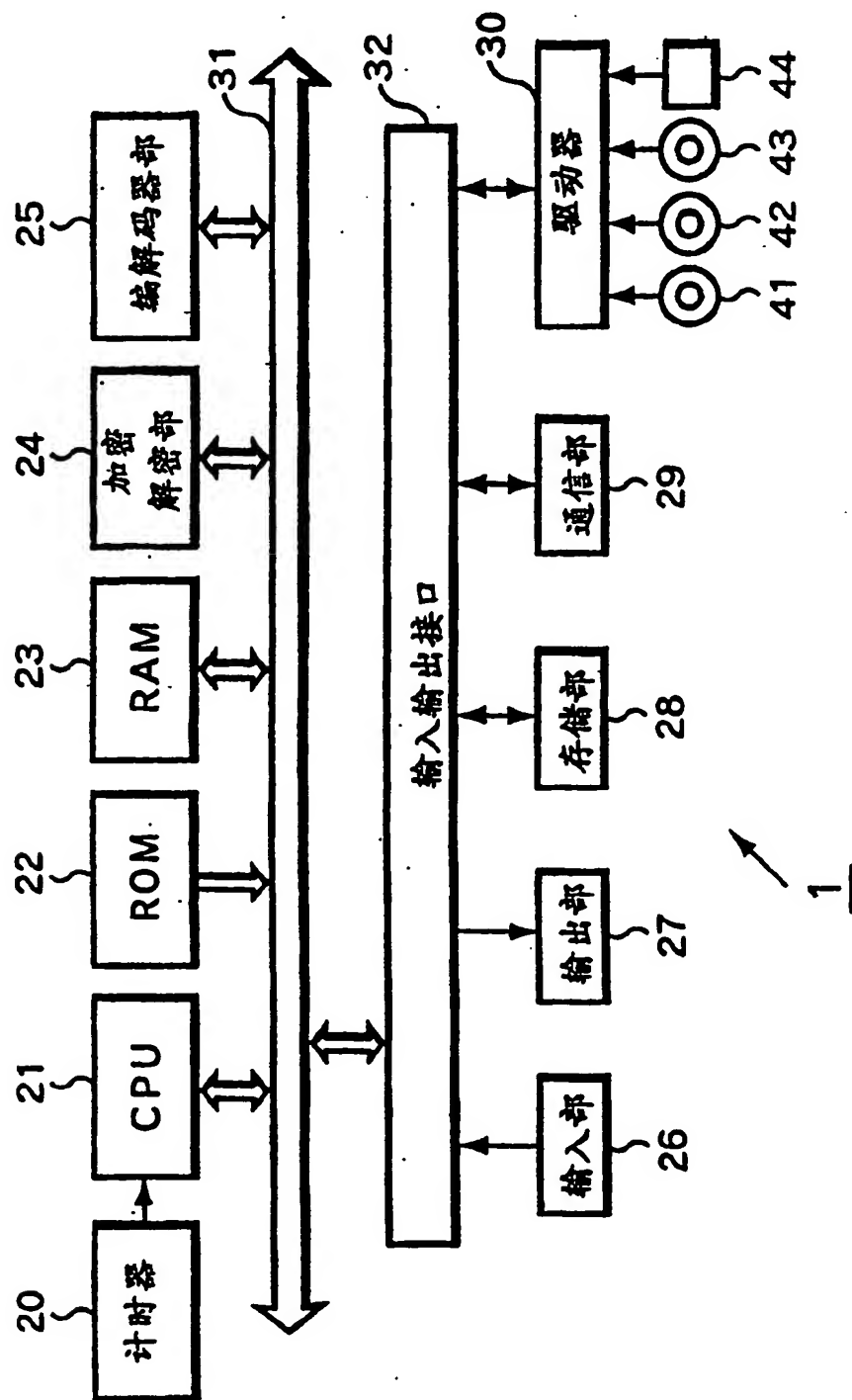


图 3

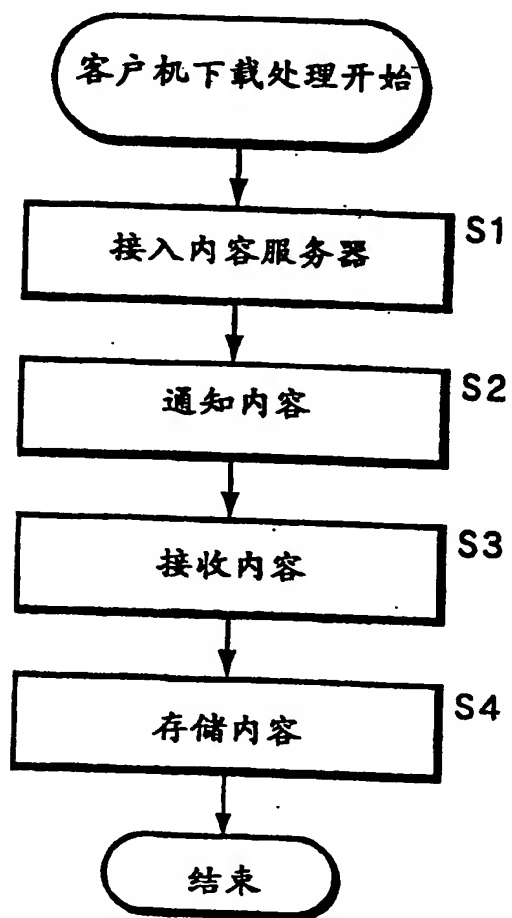


图 4

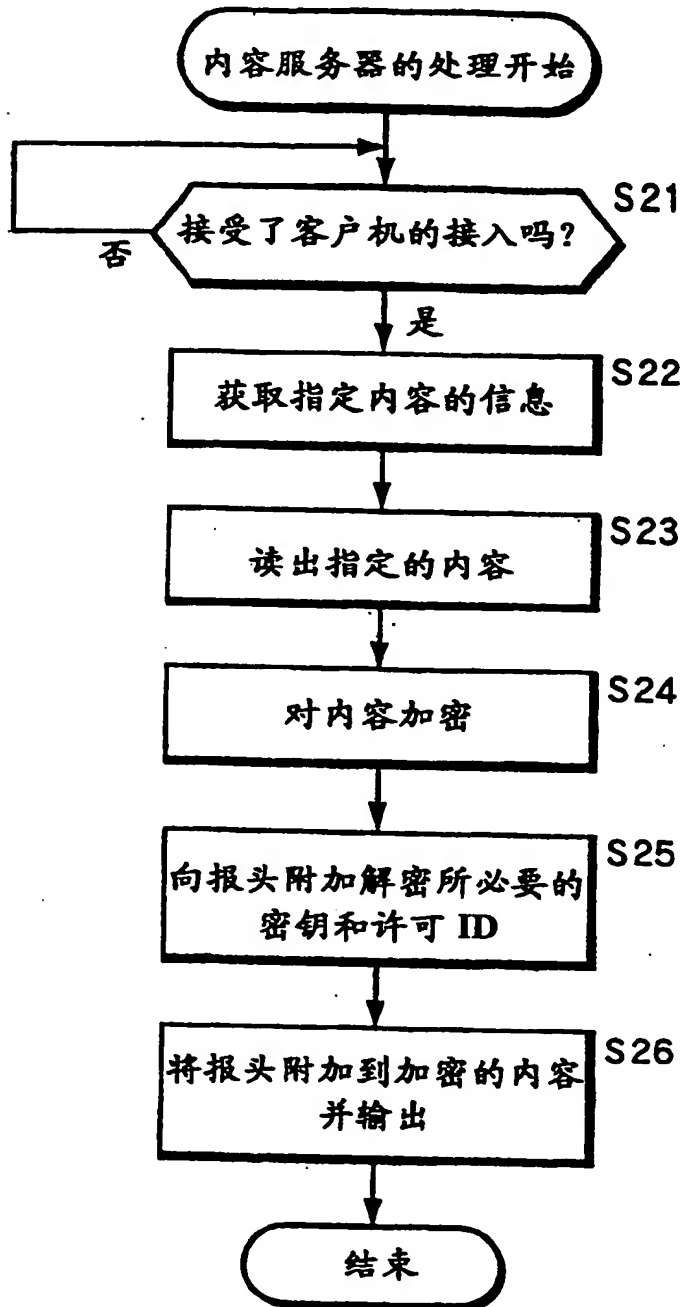


图 5

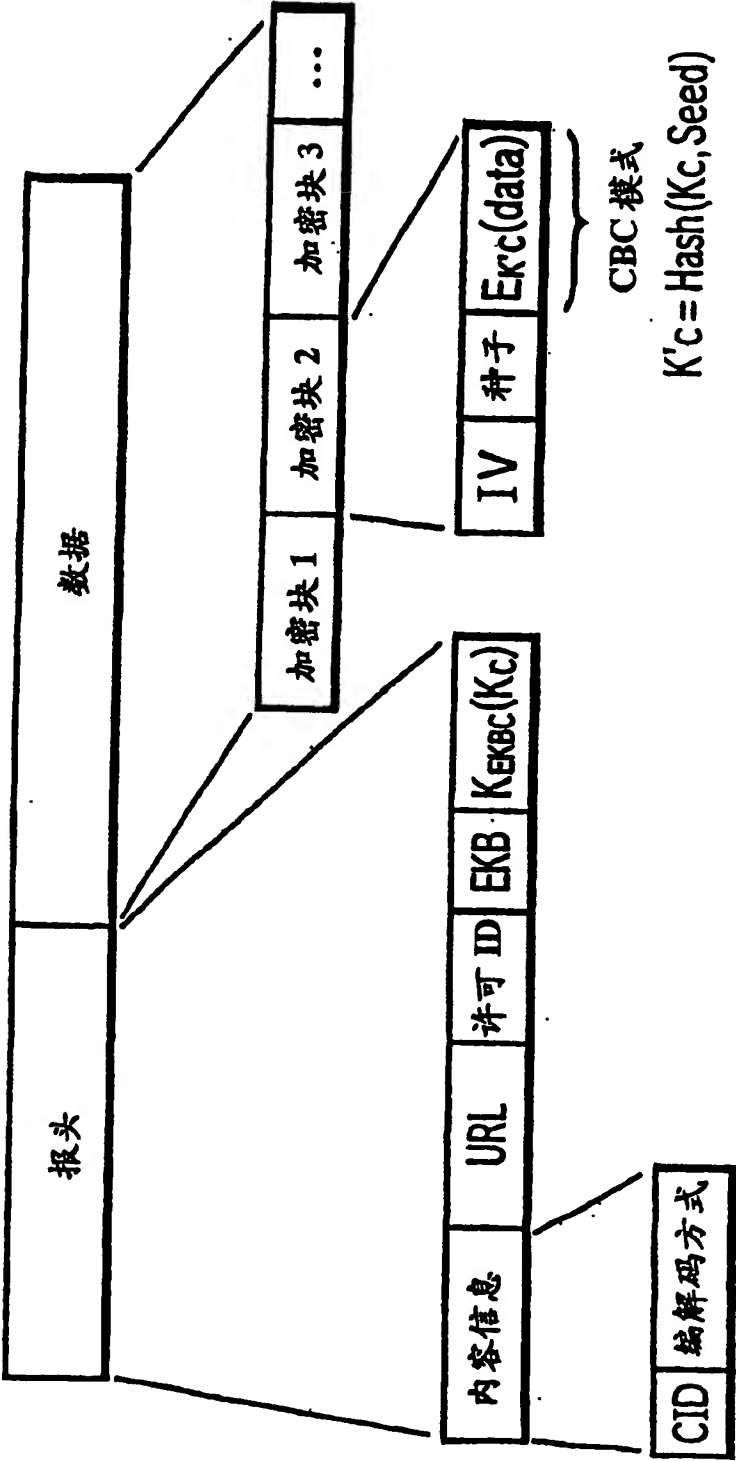


图 6

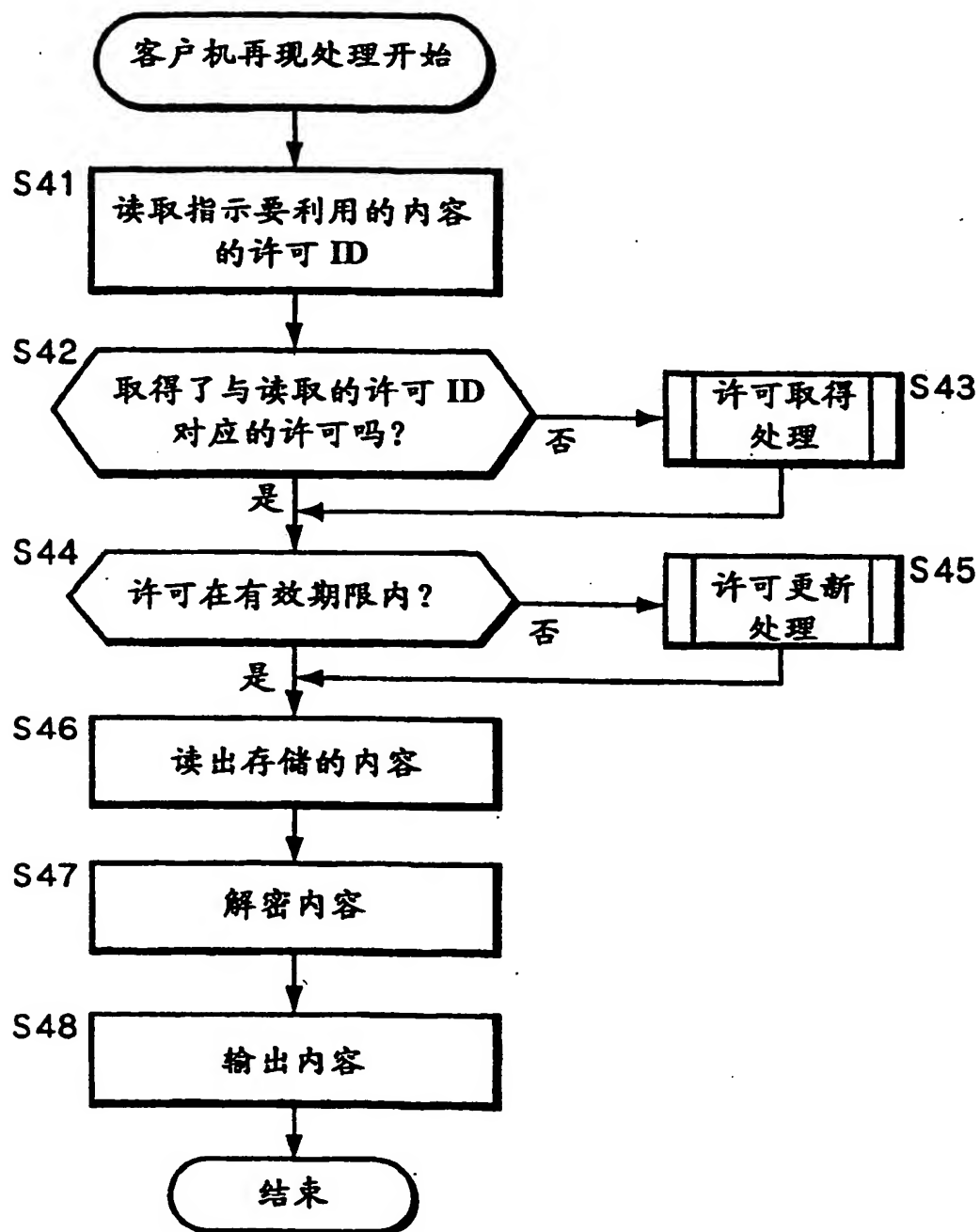


图 7

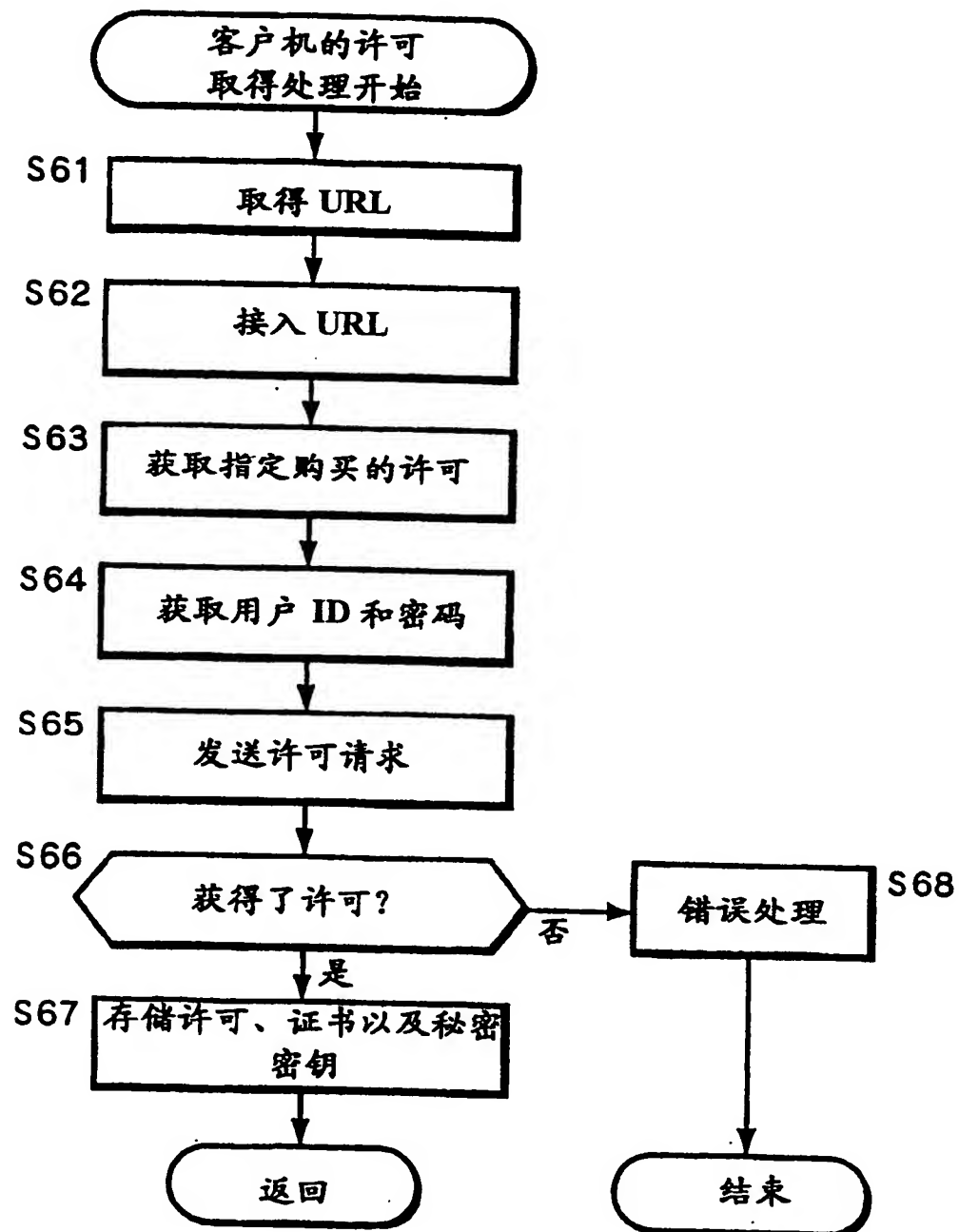


图 8

许可 ID
生成日期时间
有效期限
使用条件
叶 ID
电子署名
许可

图 9

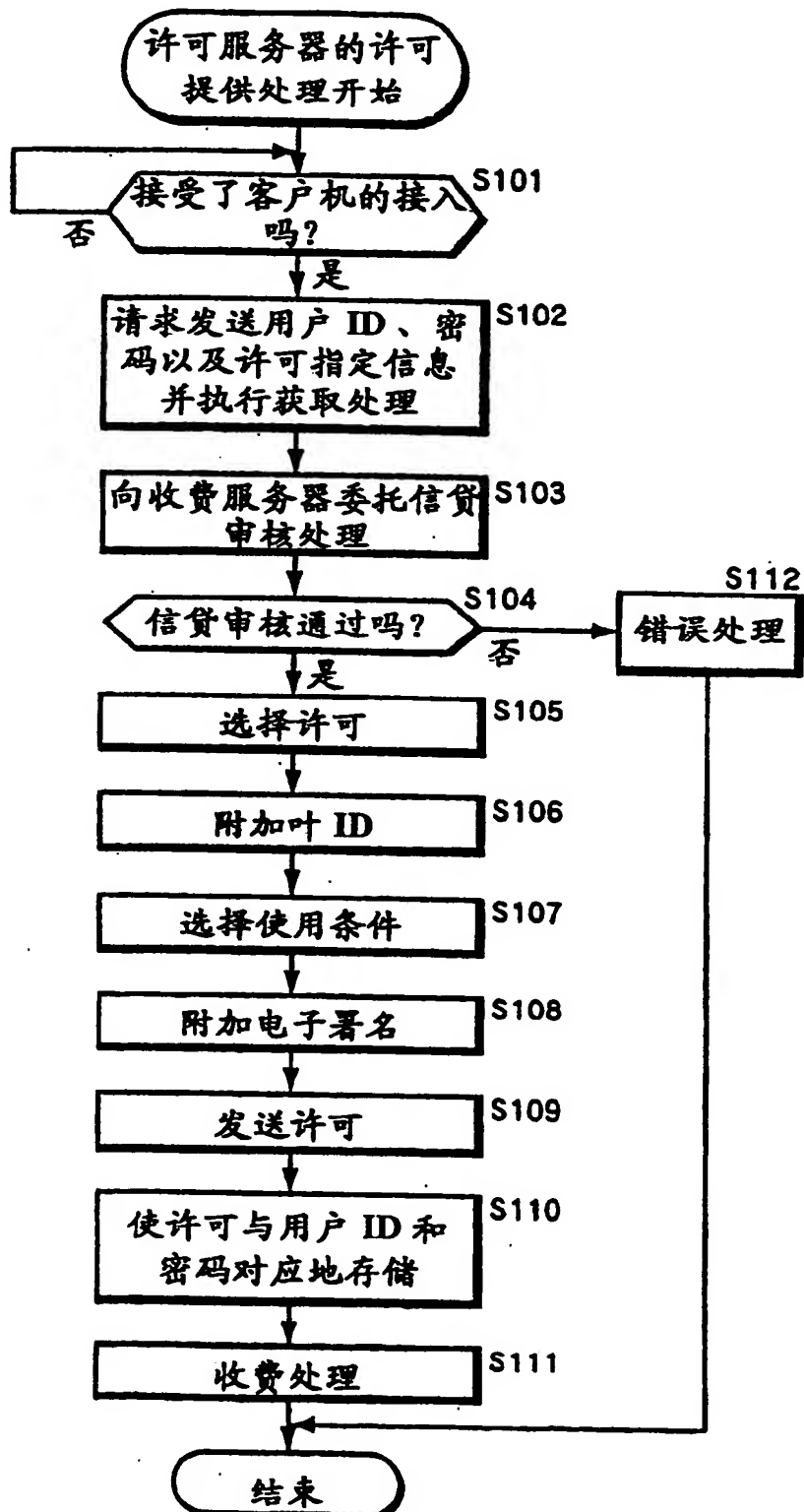


图 10

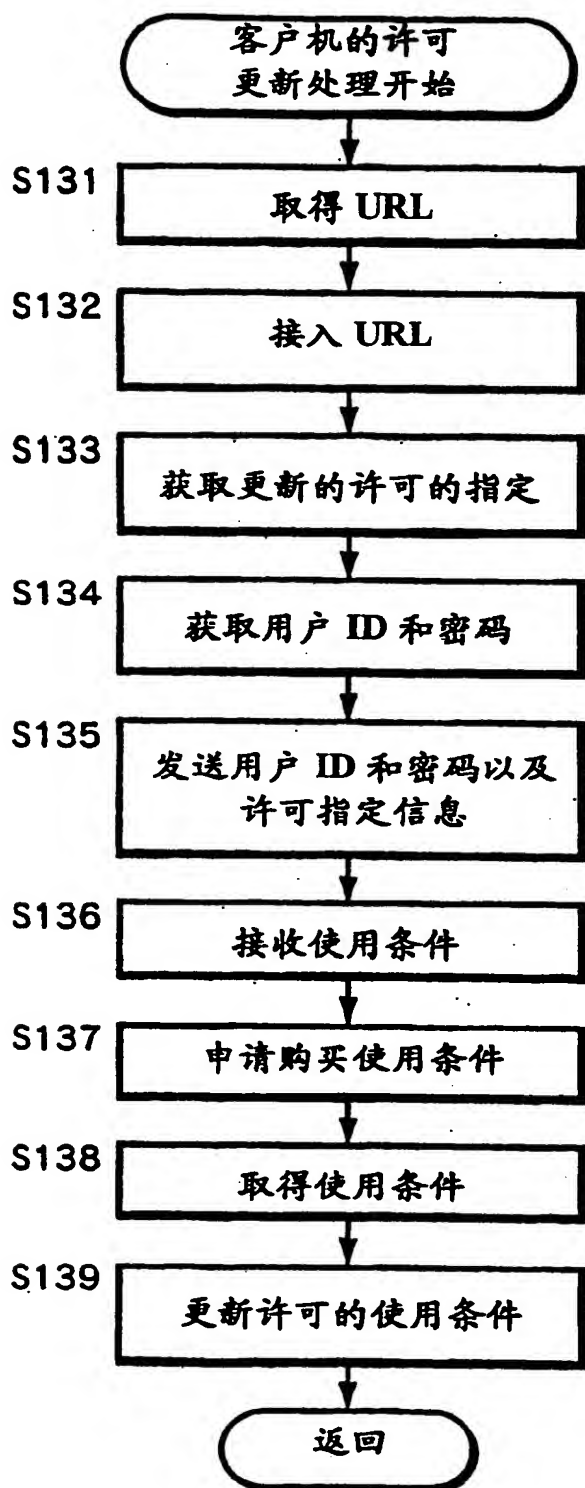
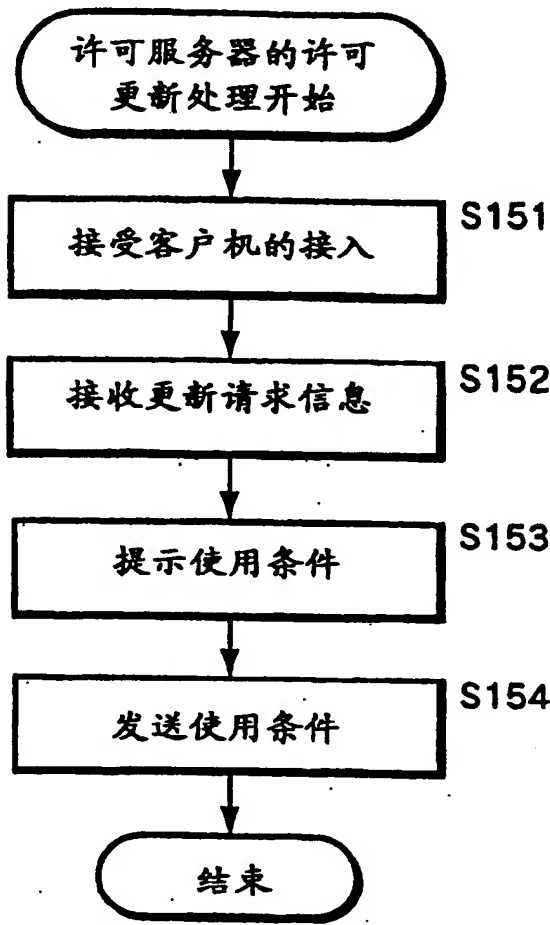


图 11



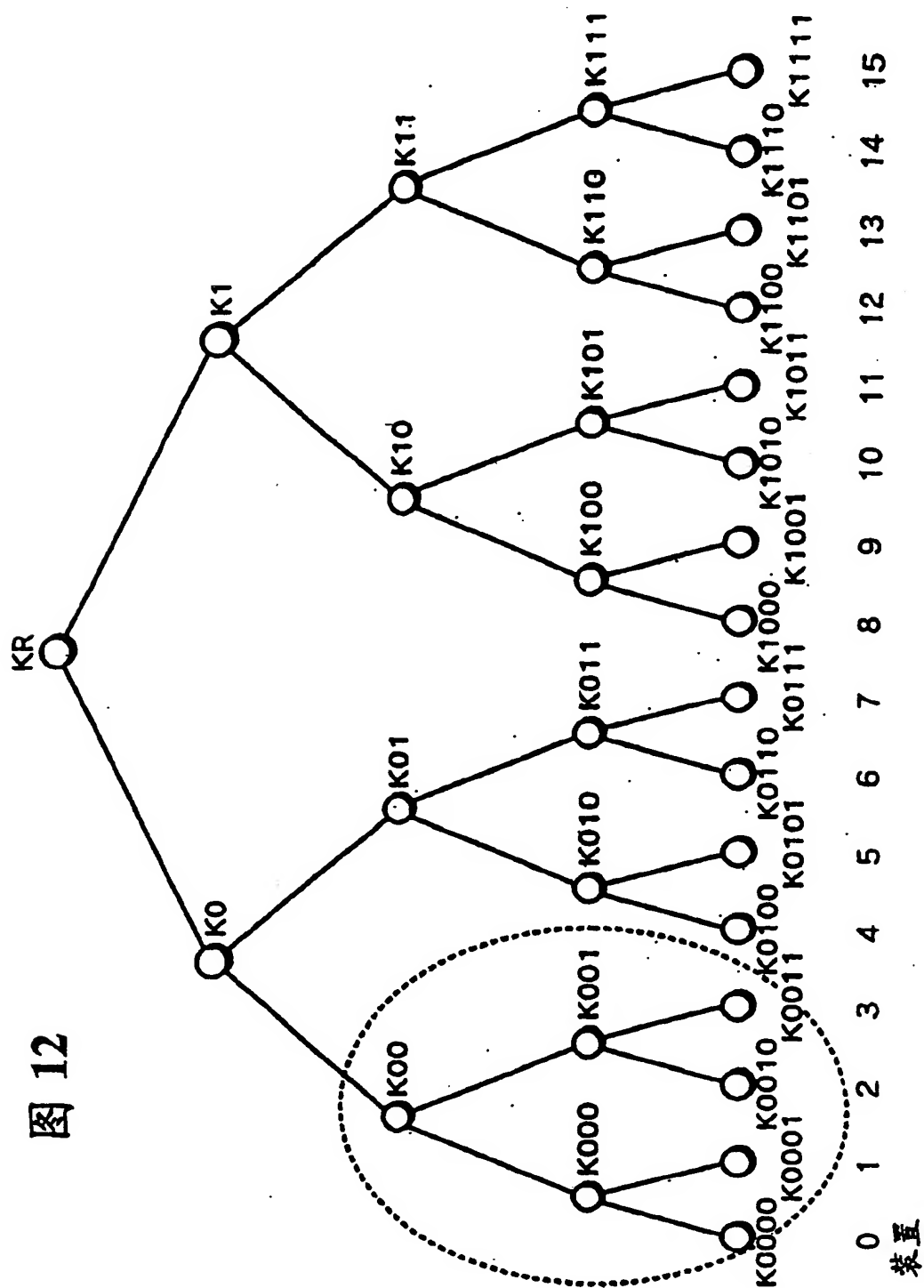


图 13

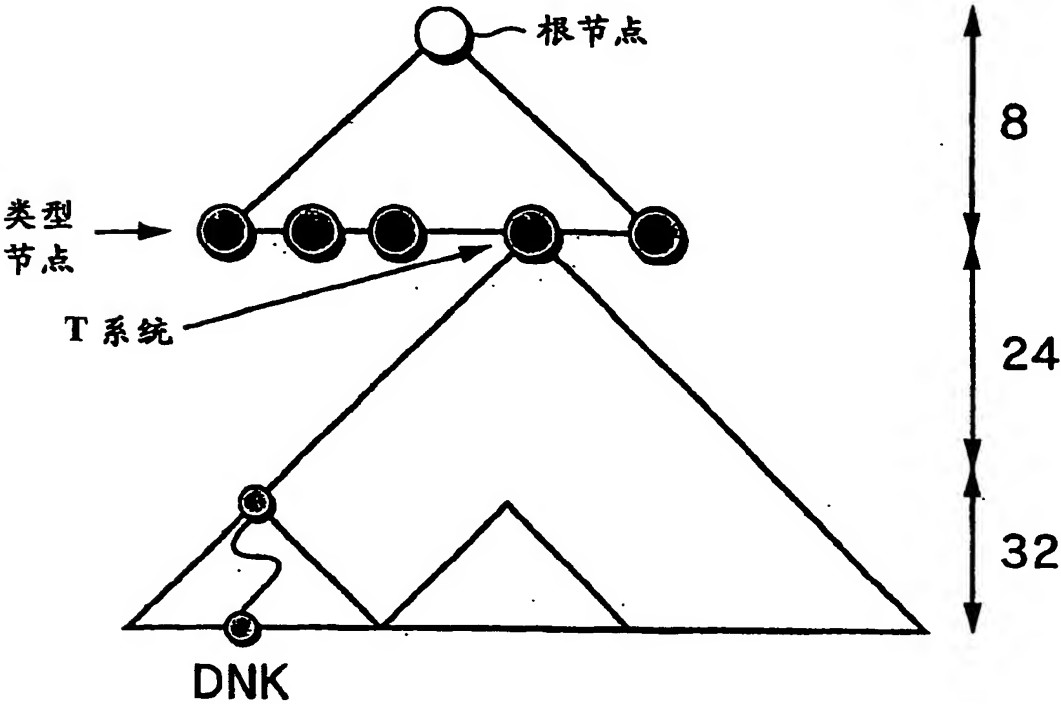


图 14

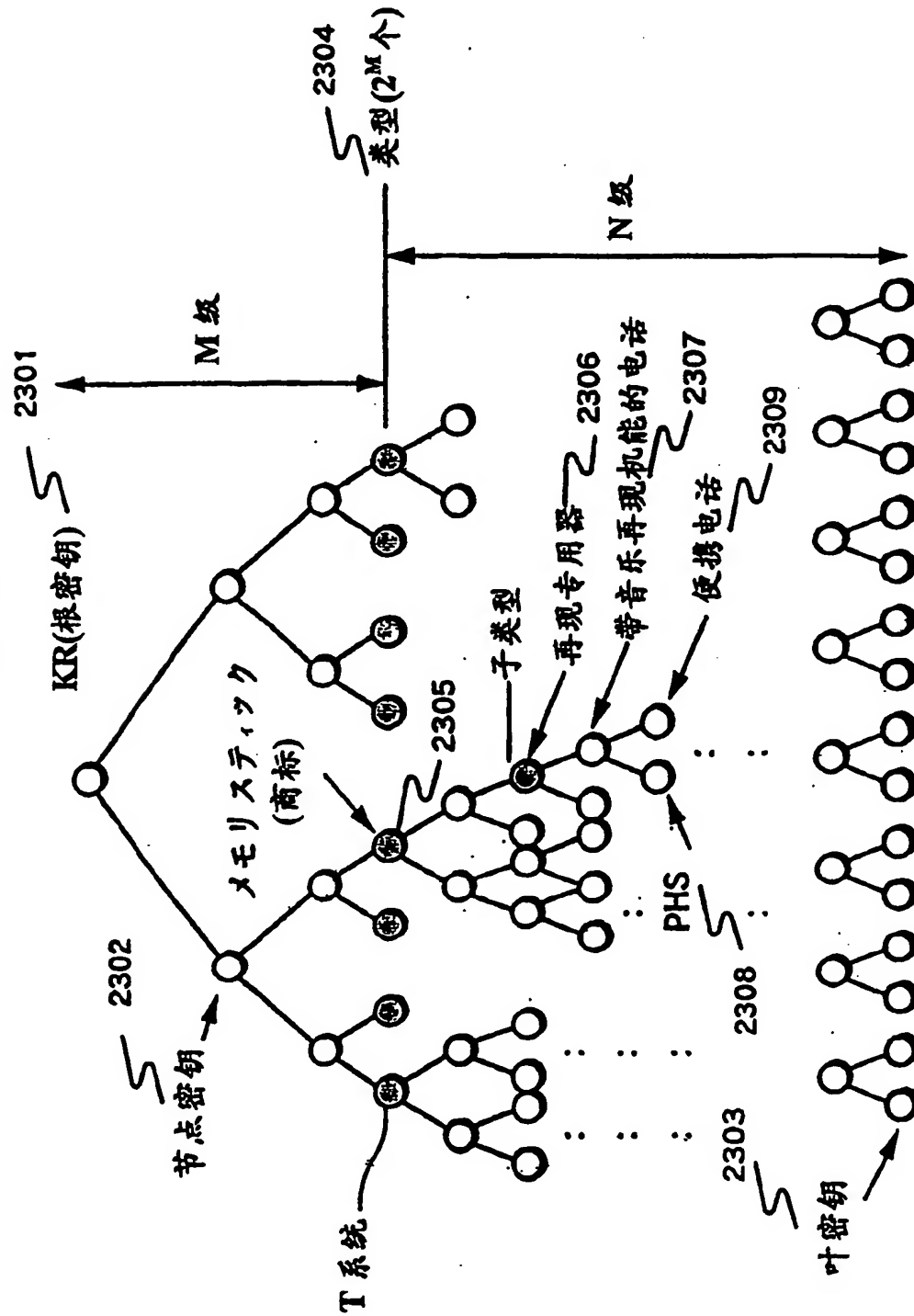


图 15A

版本(Version) t	
索引	加密密钥
0	$\text{Enc}(K(t)0, K(t)R)$
00	$\text{Enc}(K(t)00, K(t)0)$
000	$\text{Enc}(K000, K(t)00)$
001	$\text{Enc}(K(t)001, K(t)00)$
0010	$\text{Enc}(K0010, K(t)001)$

版本(Version) t	
索引	加密密钥
000	$\text{Enc}(K000, K(t)00)$
001	$\text{Enc}(K(t)001, K(t)00)$
0010	$\text{Enc}(K0010, K(t)001)$

图 15B

图 16

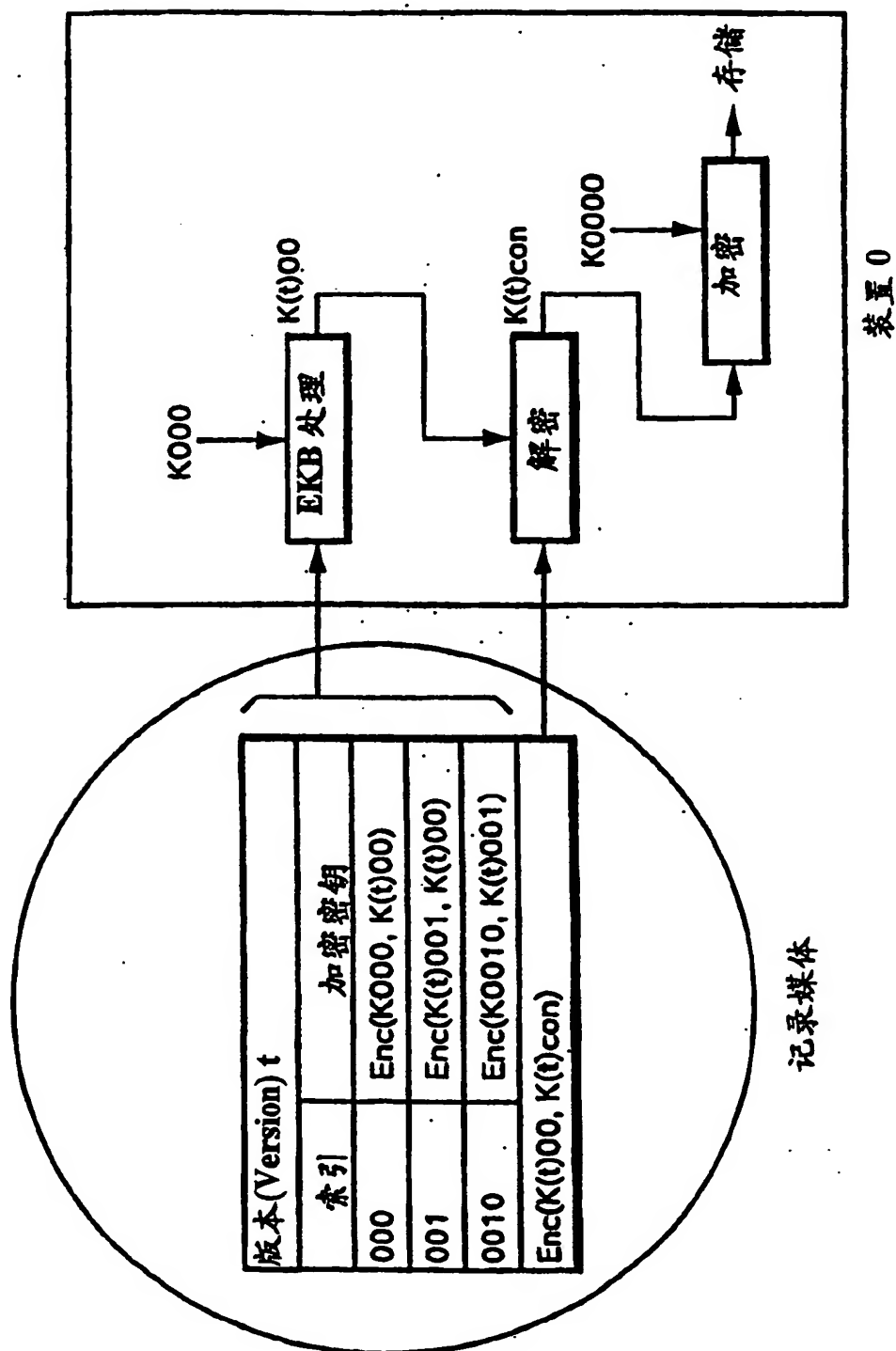


图 17

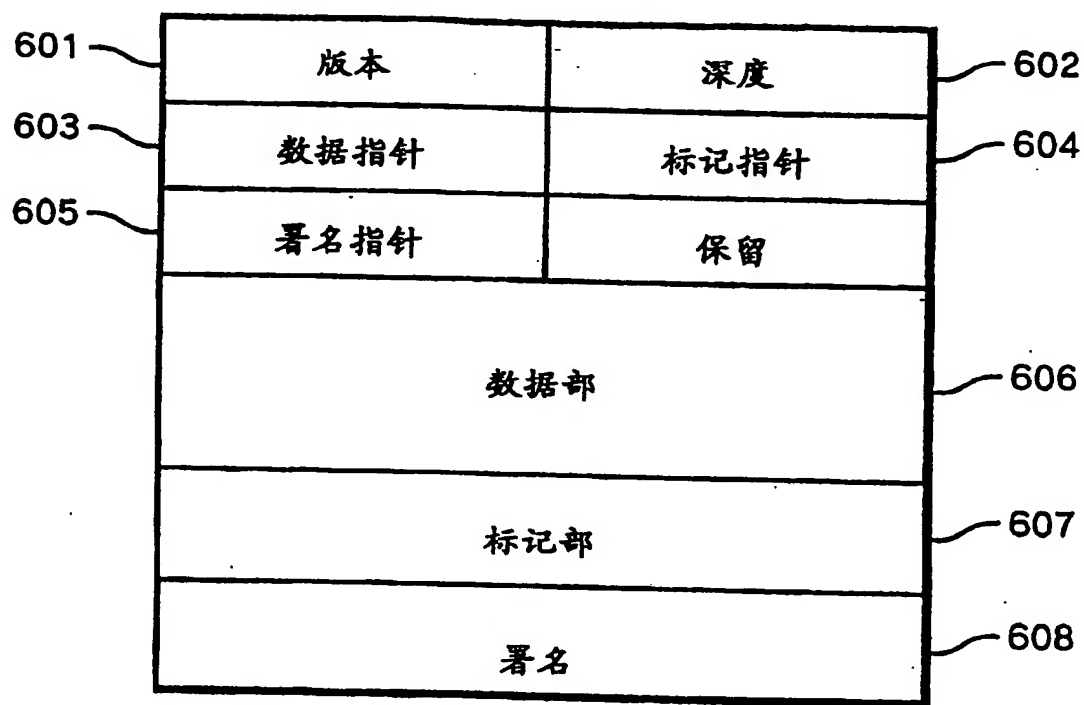


图 18

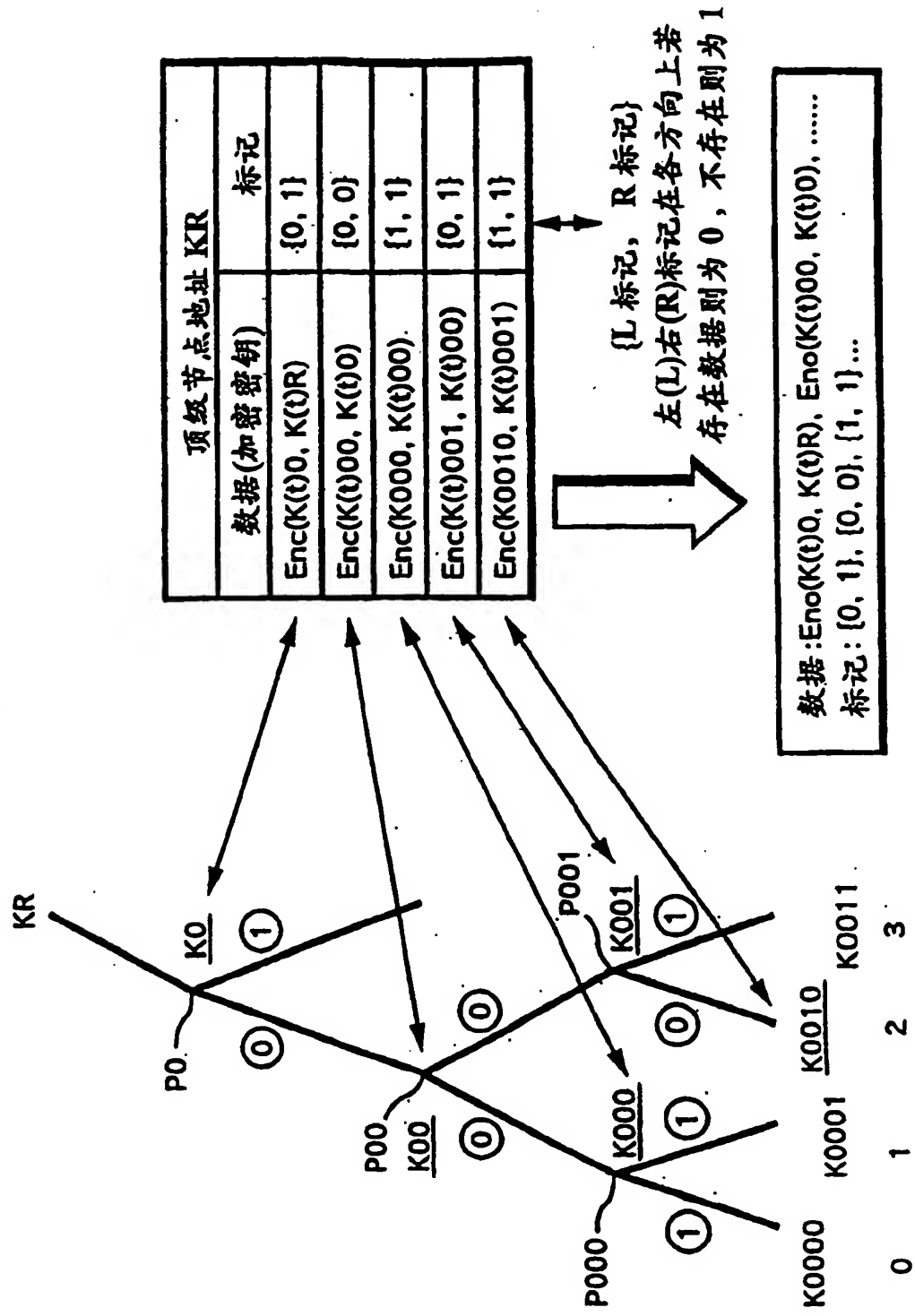
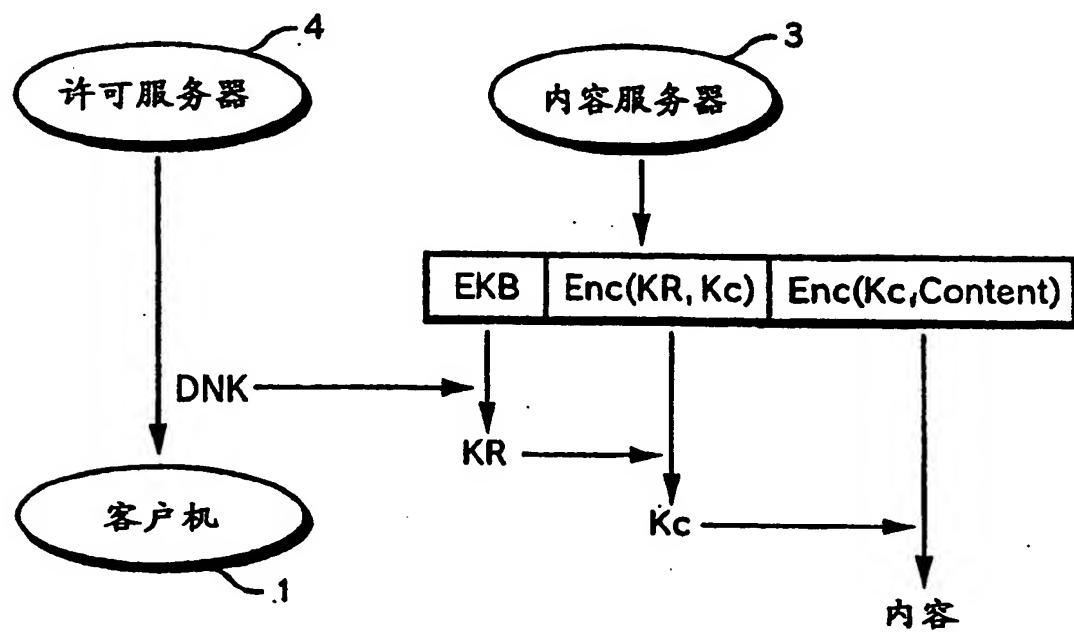


图 19



EKB

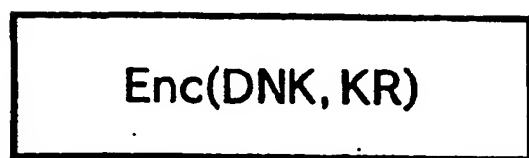


图 20

图 21

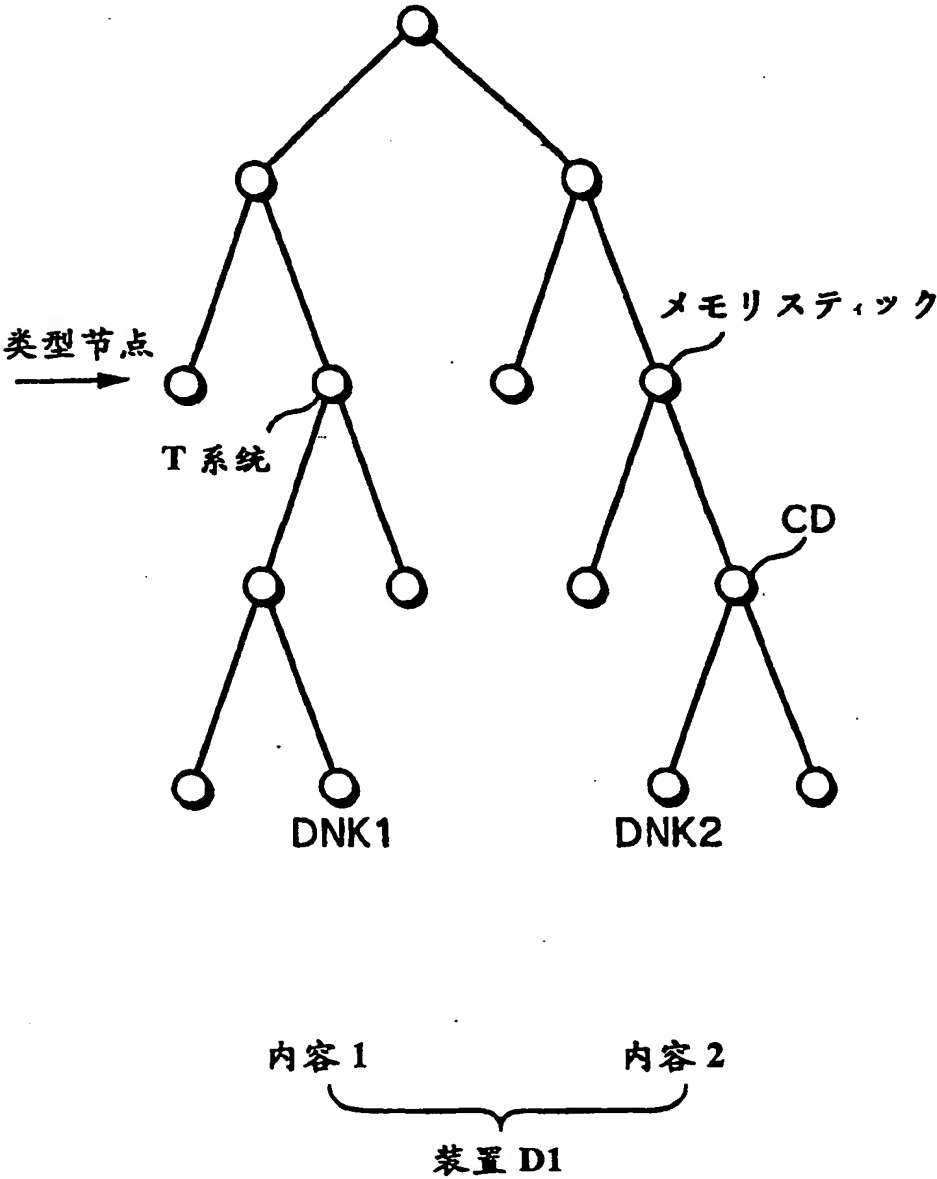


图 22

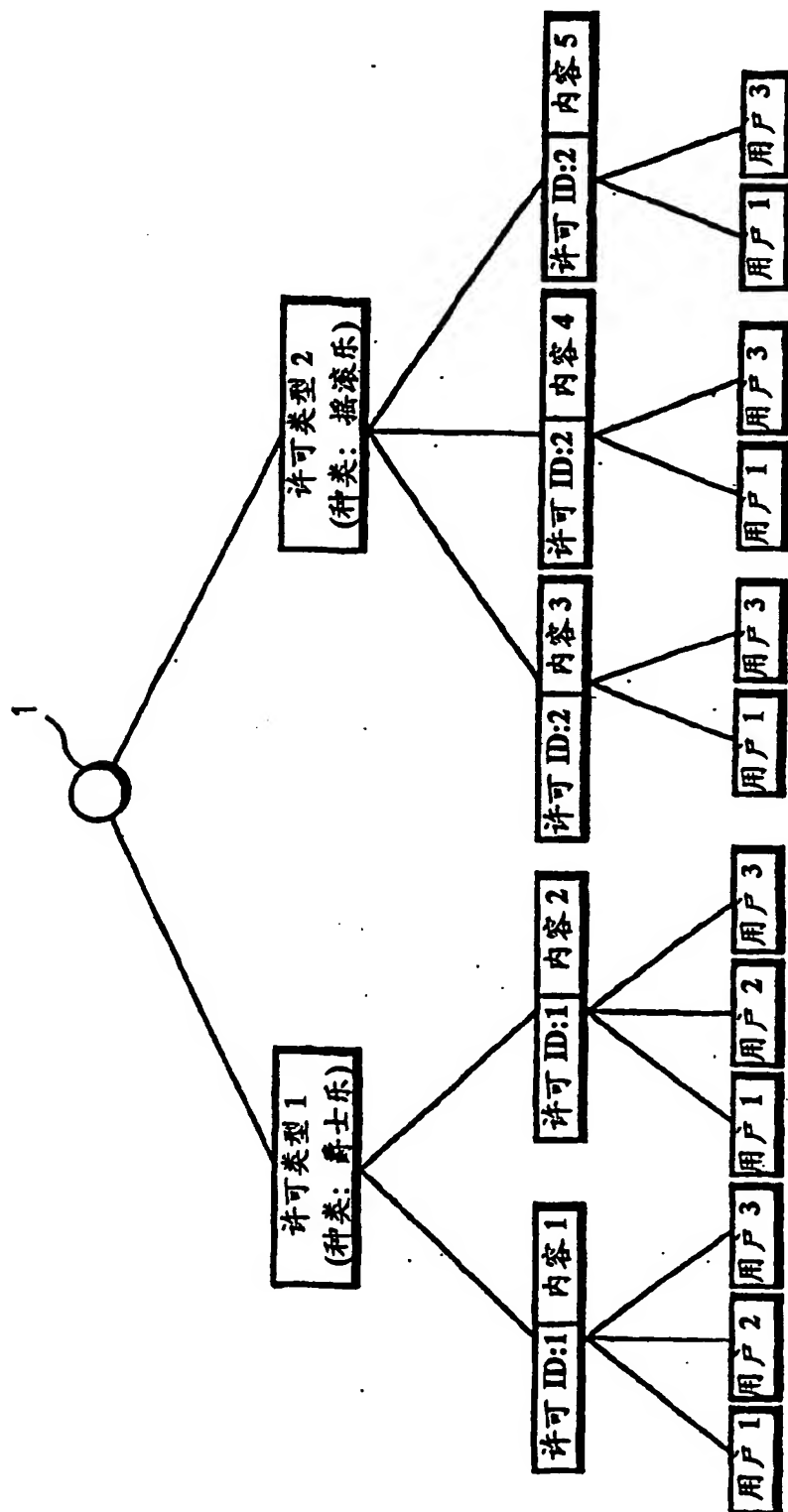


图 23

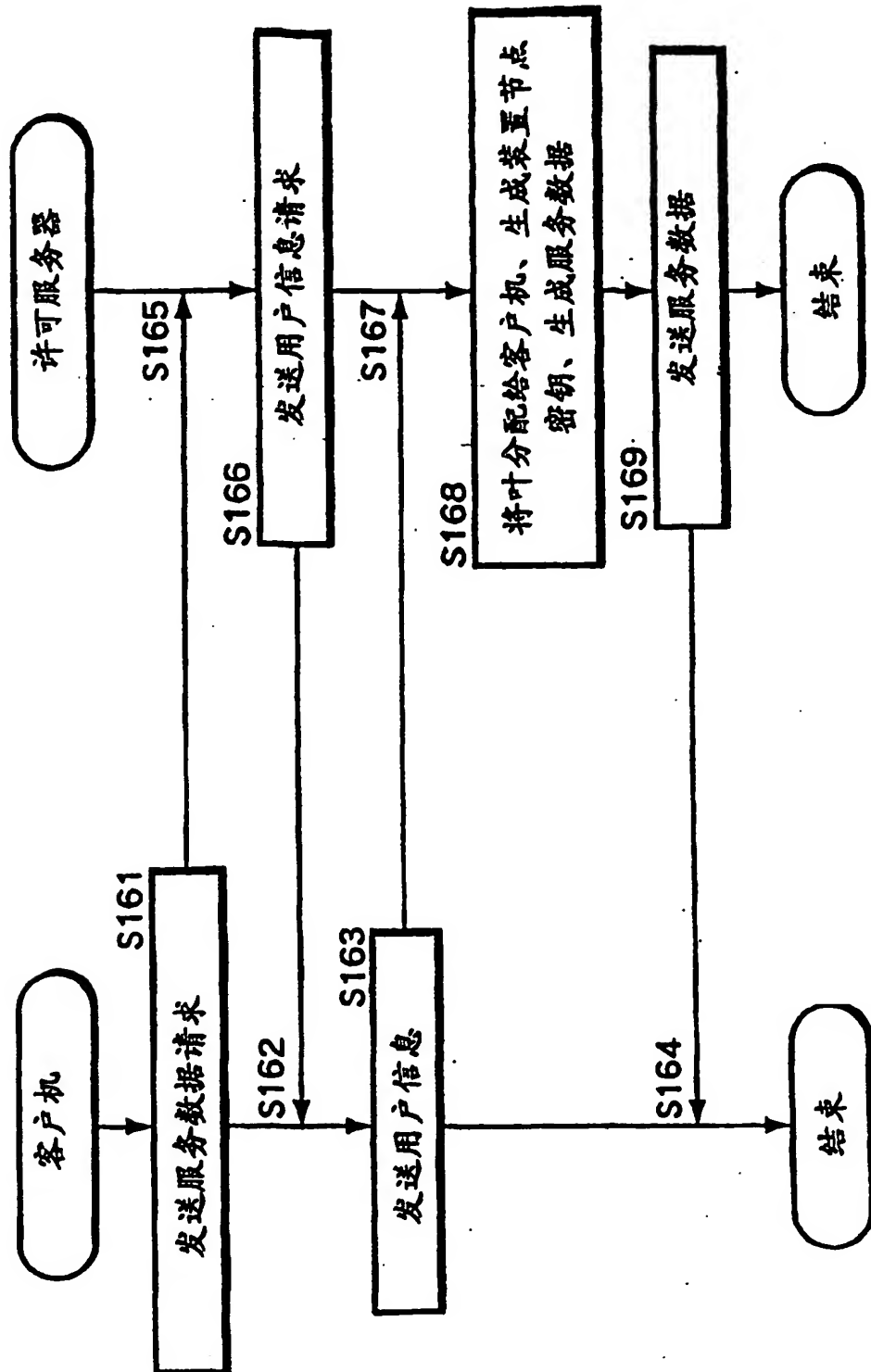


图 24

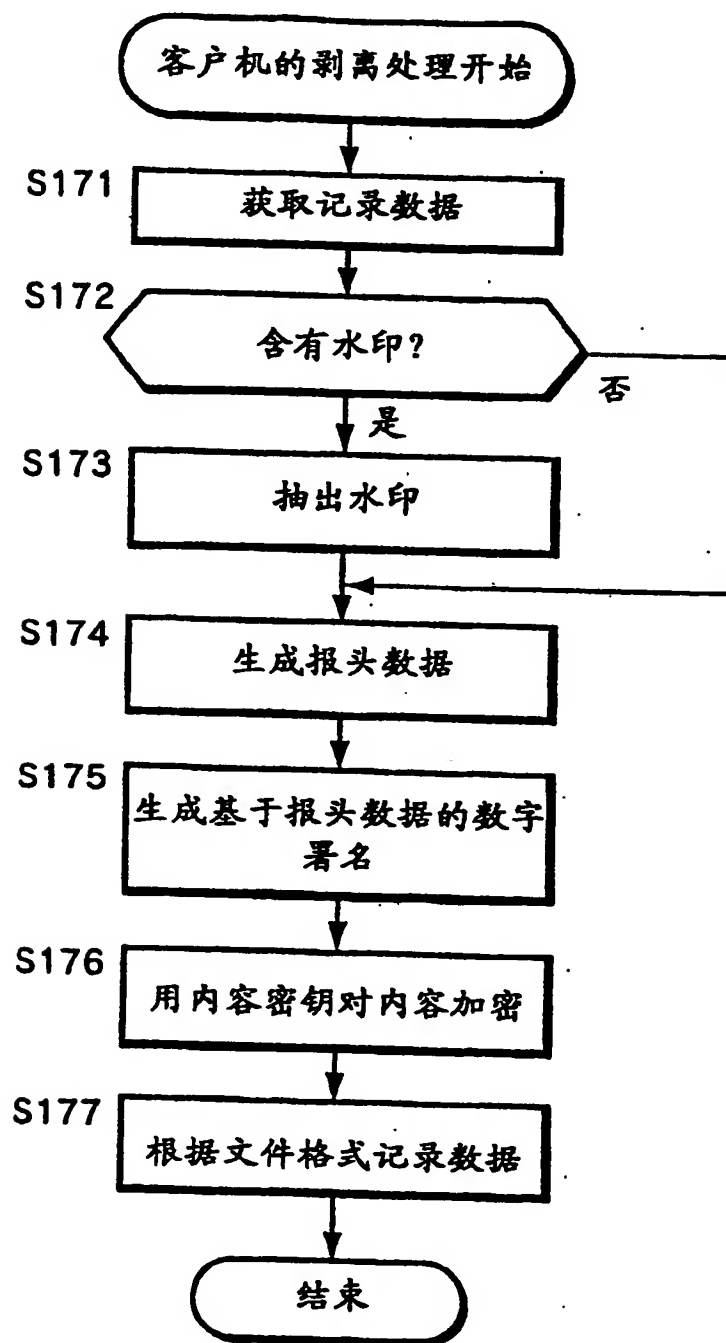


图 25

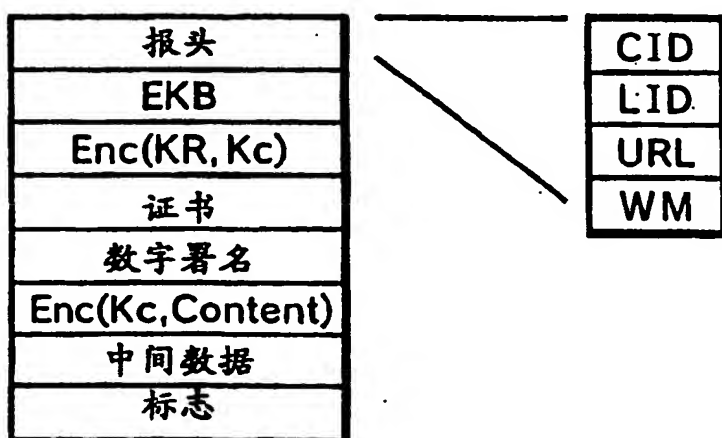
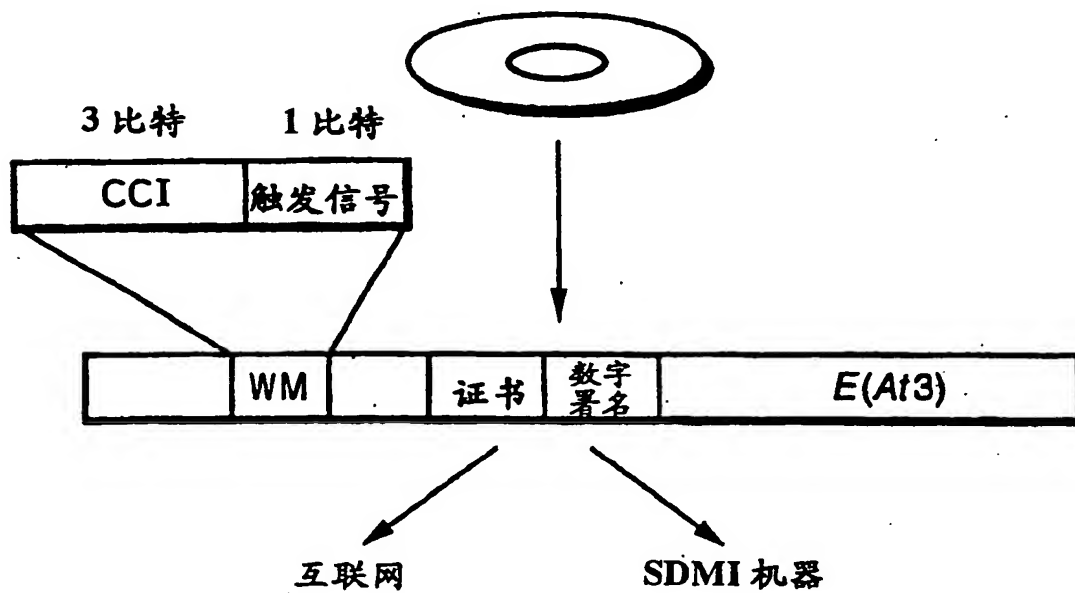


图 26

图 27

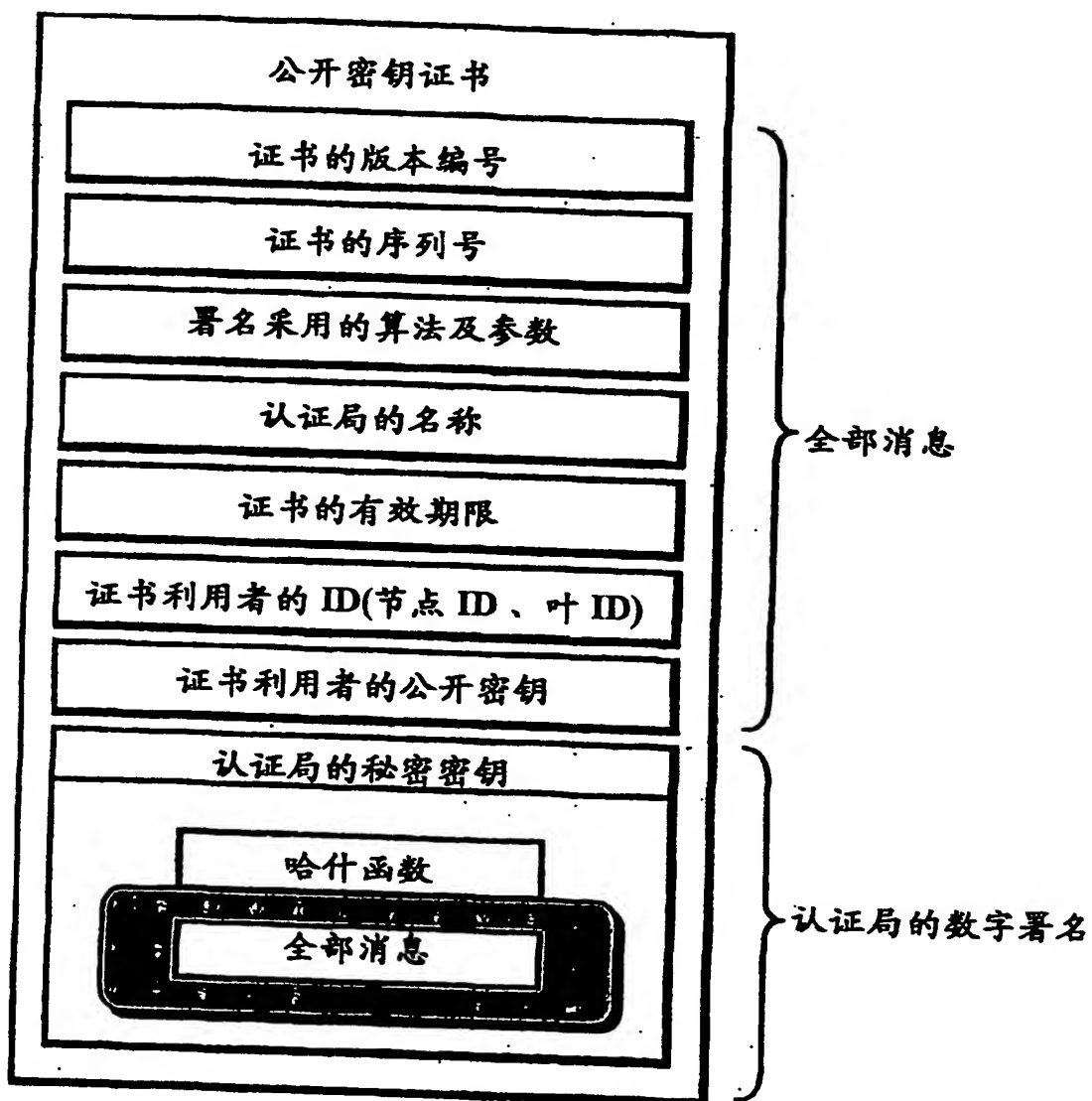


图 28

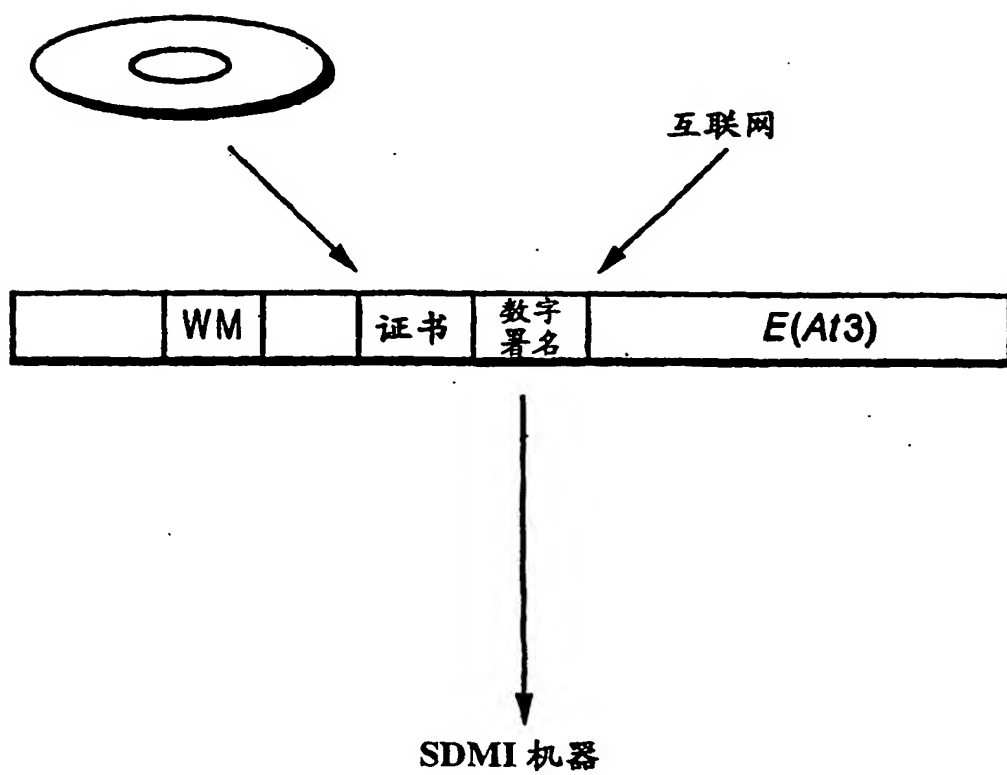


图 29

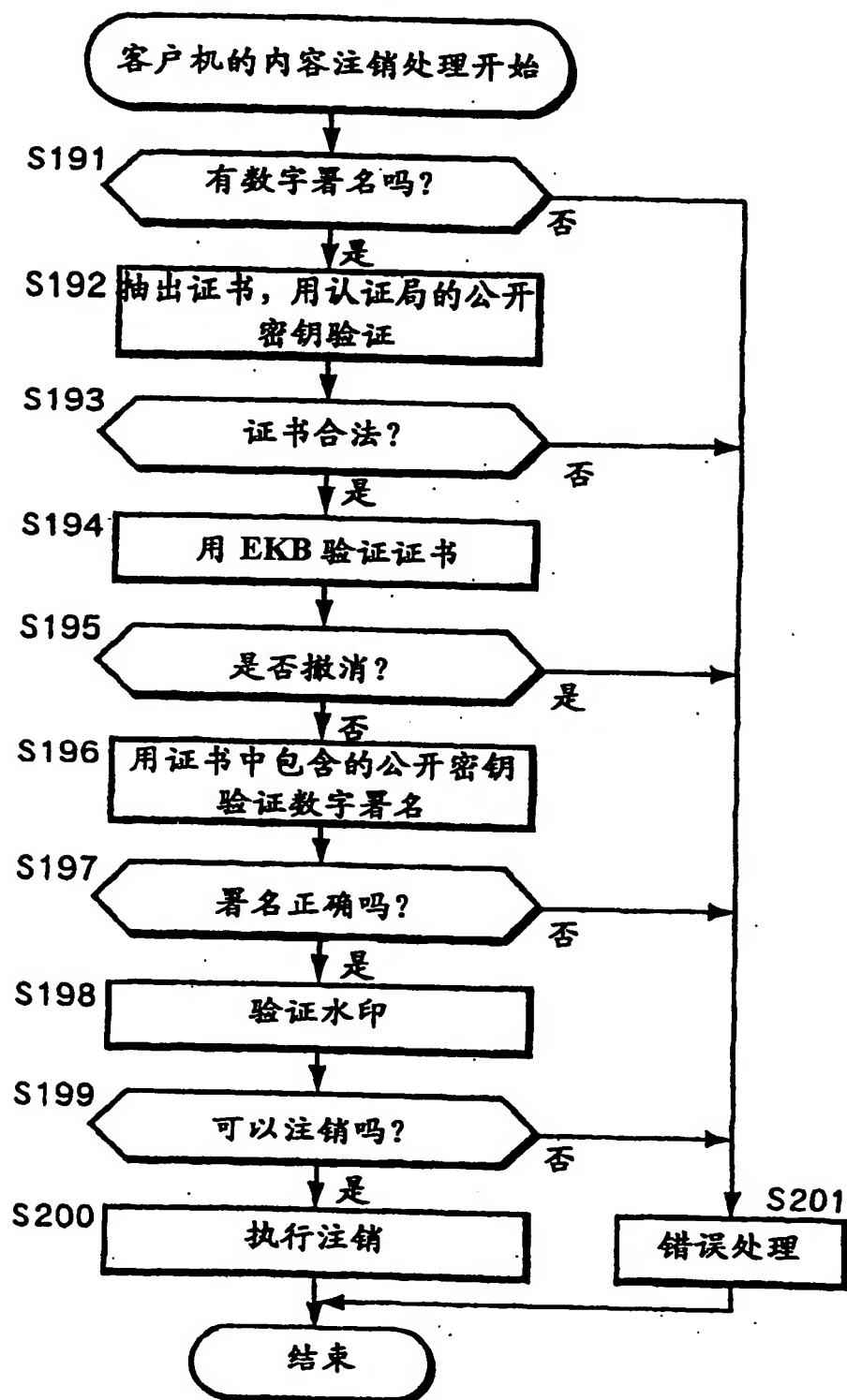


图 30

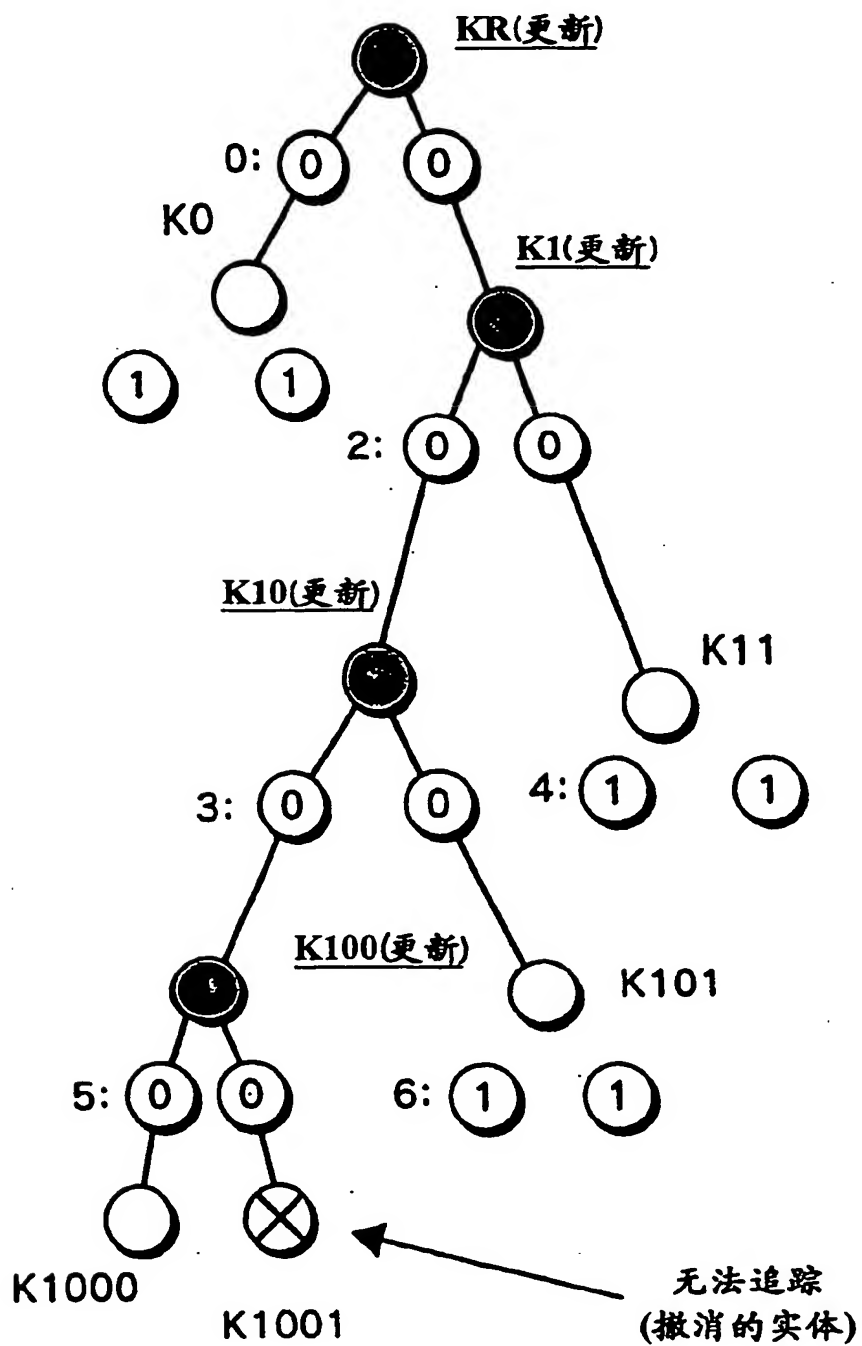
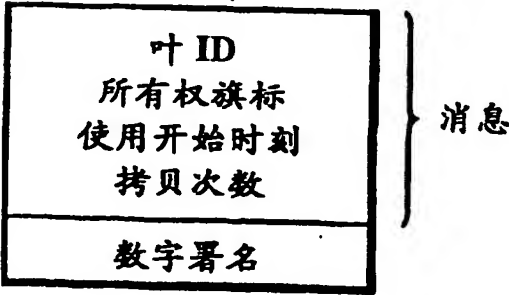


图 31

数据 (加密密钥)	Enc(K0, K(t)R), Enc(K(t)1, K(t)R) Enc(K(t)10, K(t)1), Enc(K11, K(t)1) Enc(K(t)100, K(t)10), Enc(K101, K(t)10) Enc(K1000, K(t)100)
标记	0: {0, 0}, 1:{1, 1}, 2:{0, 0}, 3:(0, 0) 4: {1, 1}, 5:{0, 1}, 6:{1, 1}



{L 标记, R 标记}
左(L)右(R)标记在各方向上若存在
数据则为 0, 不存在则为 1



标志

图 32

图 33

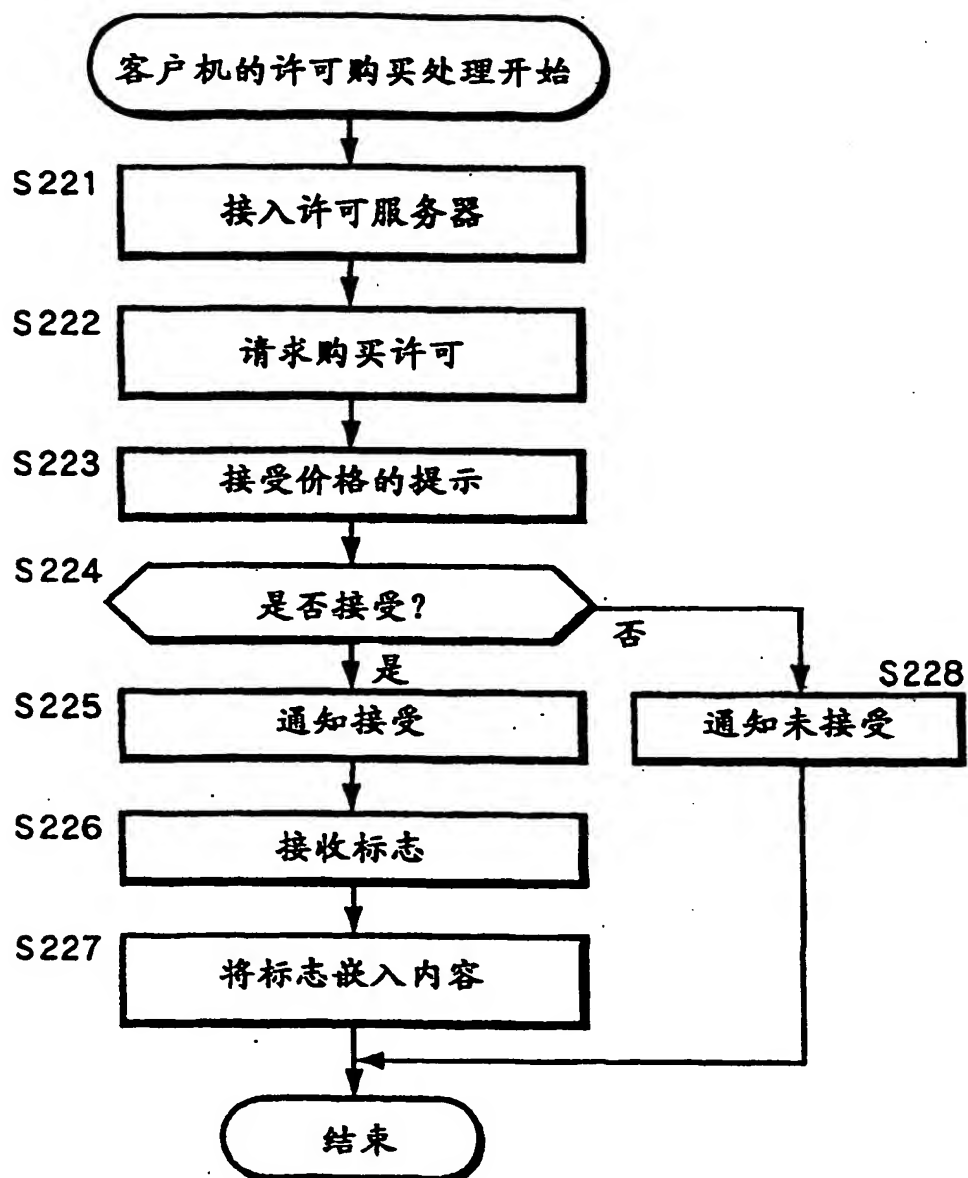


图 34

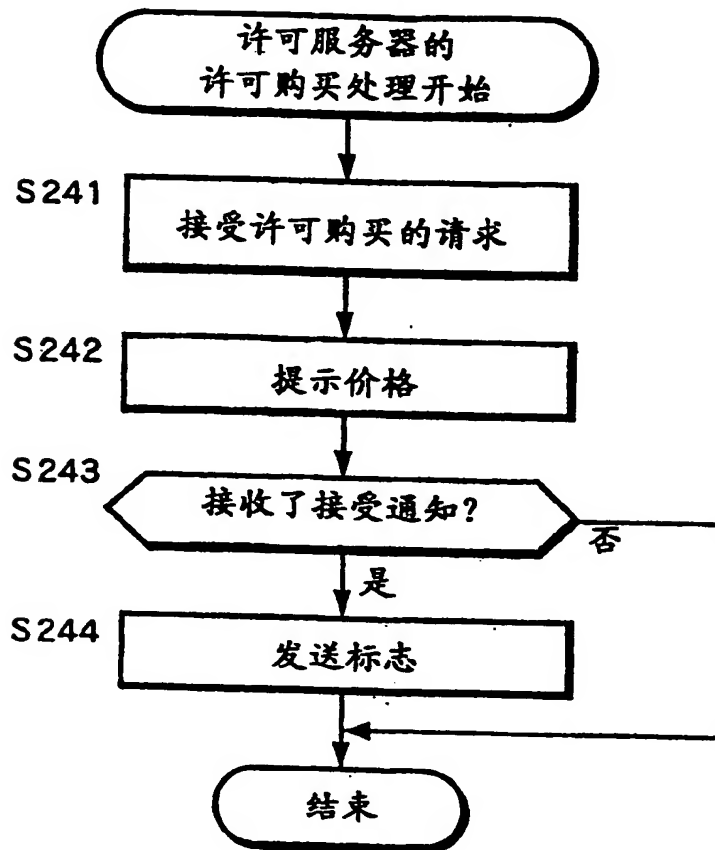


图 35

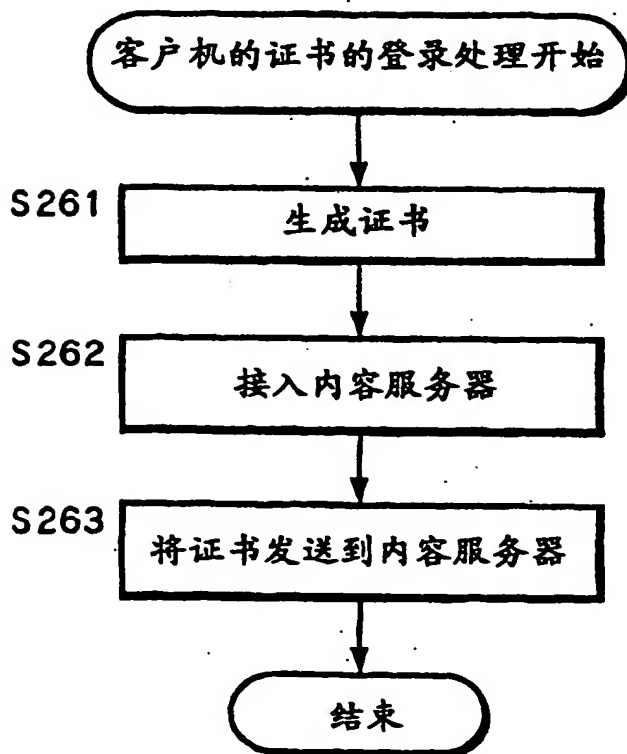
$$\text{Mark} = \{\text{LeafID}, \text{Own}, \text{Sigs}(\text{LeafID}, \text{Own})\}$$


图 36

图 37

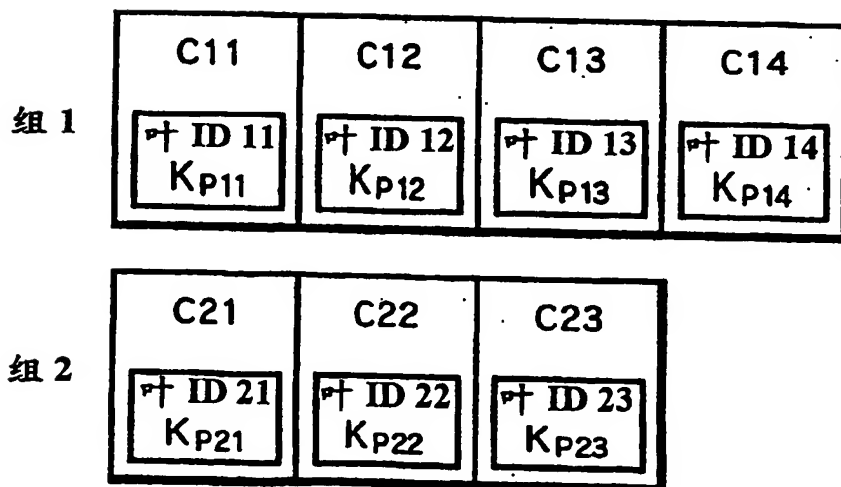
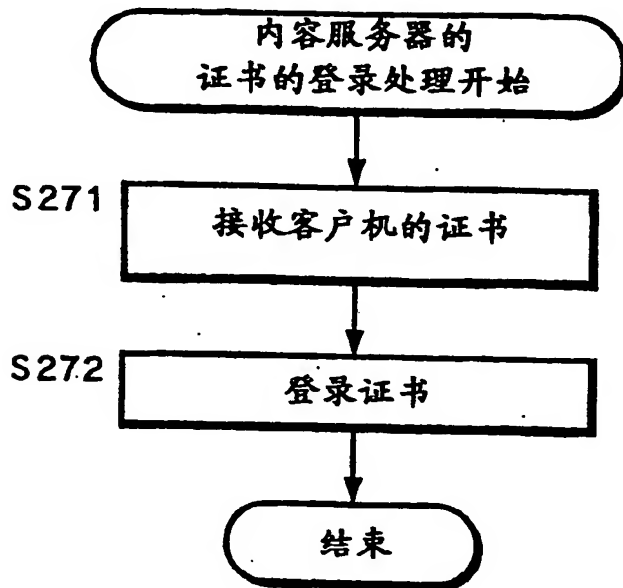
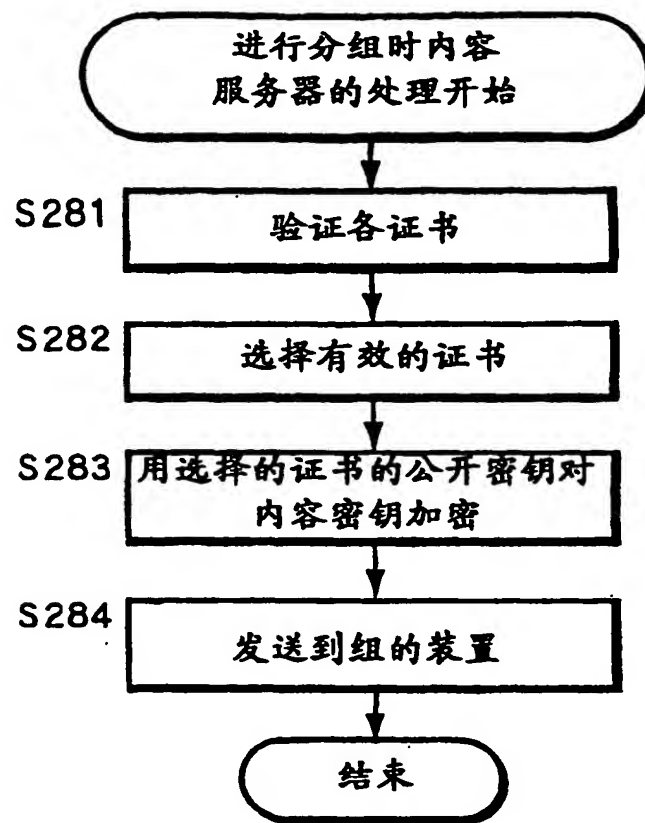


图 38

图 39



$\text{Enc}(K_{p11}, K_c), \text{Enc}(K_{p12}, K_c), \text{Enc}(K_{p13}, K_c)$

图 40

图 41

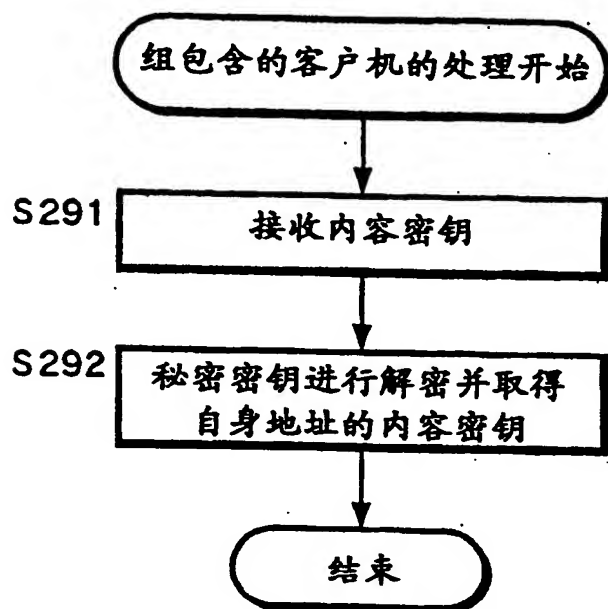


图 42

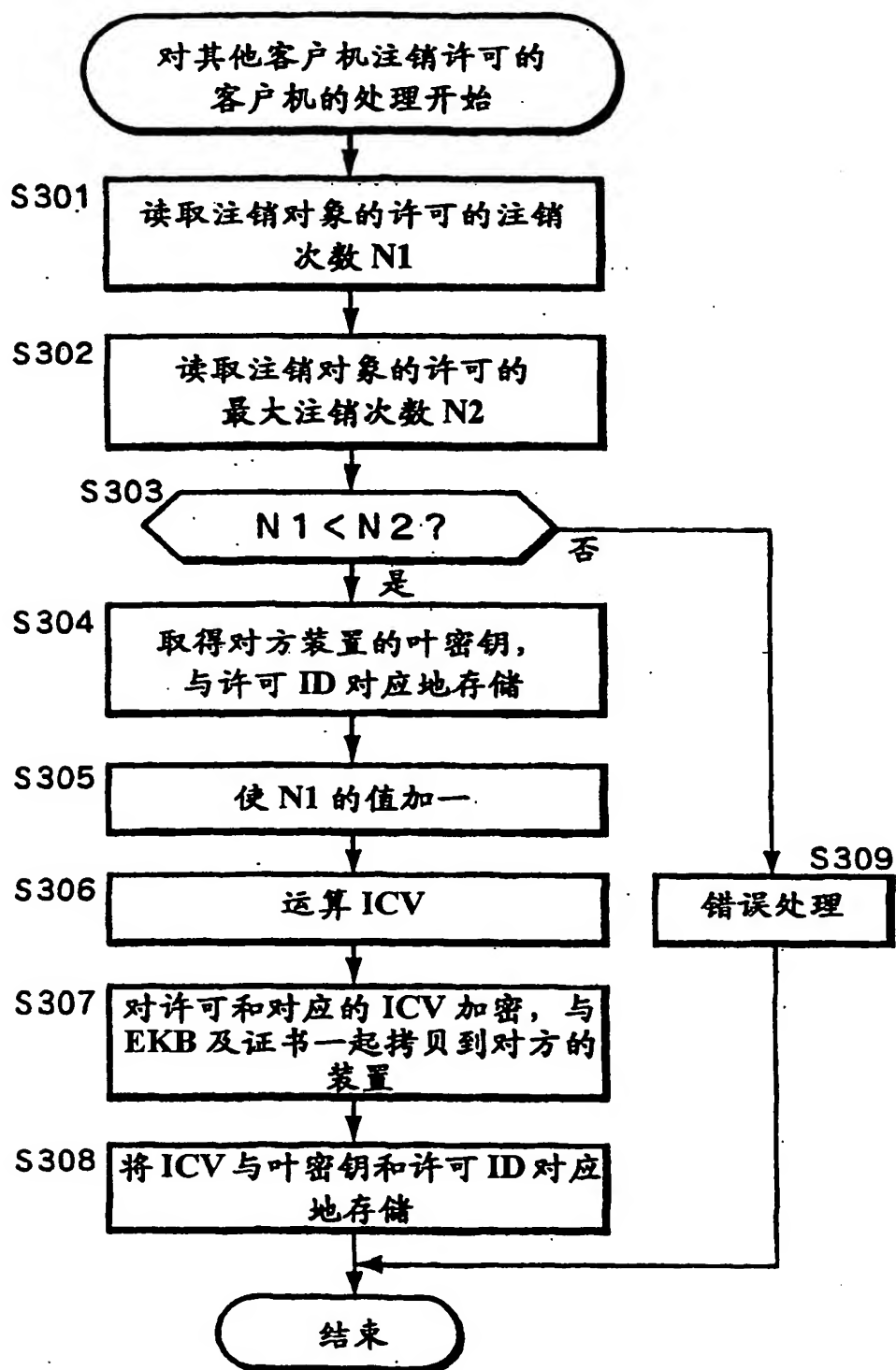


图 43

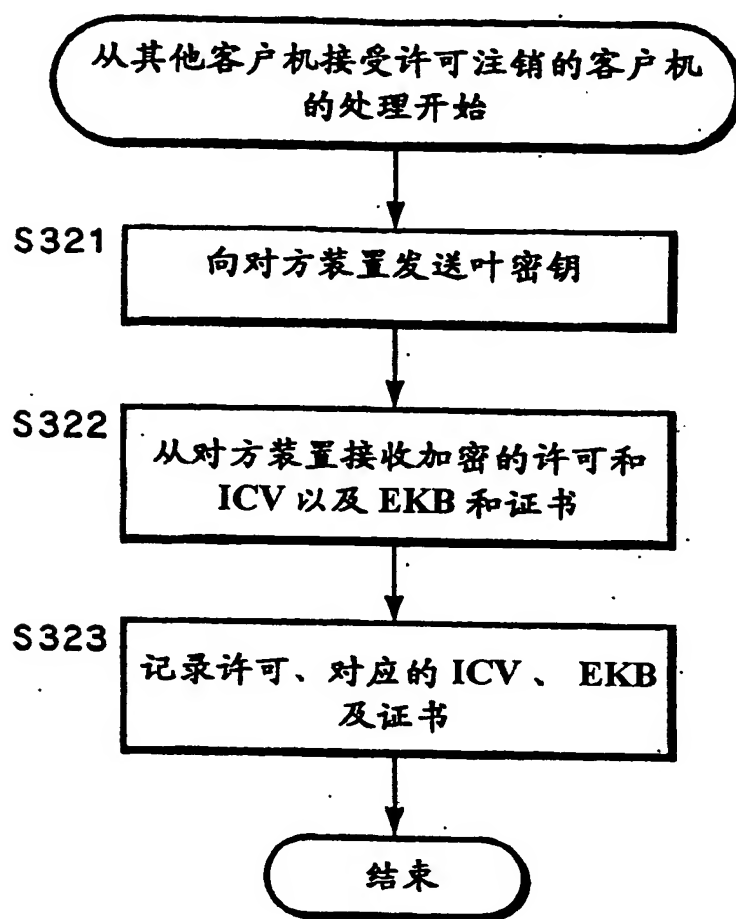


图 44

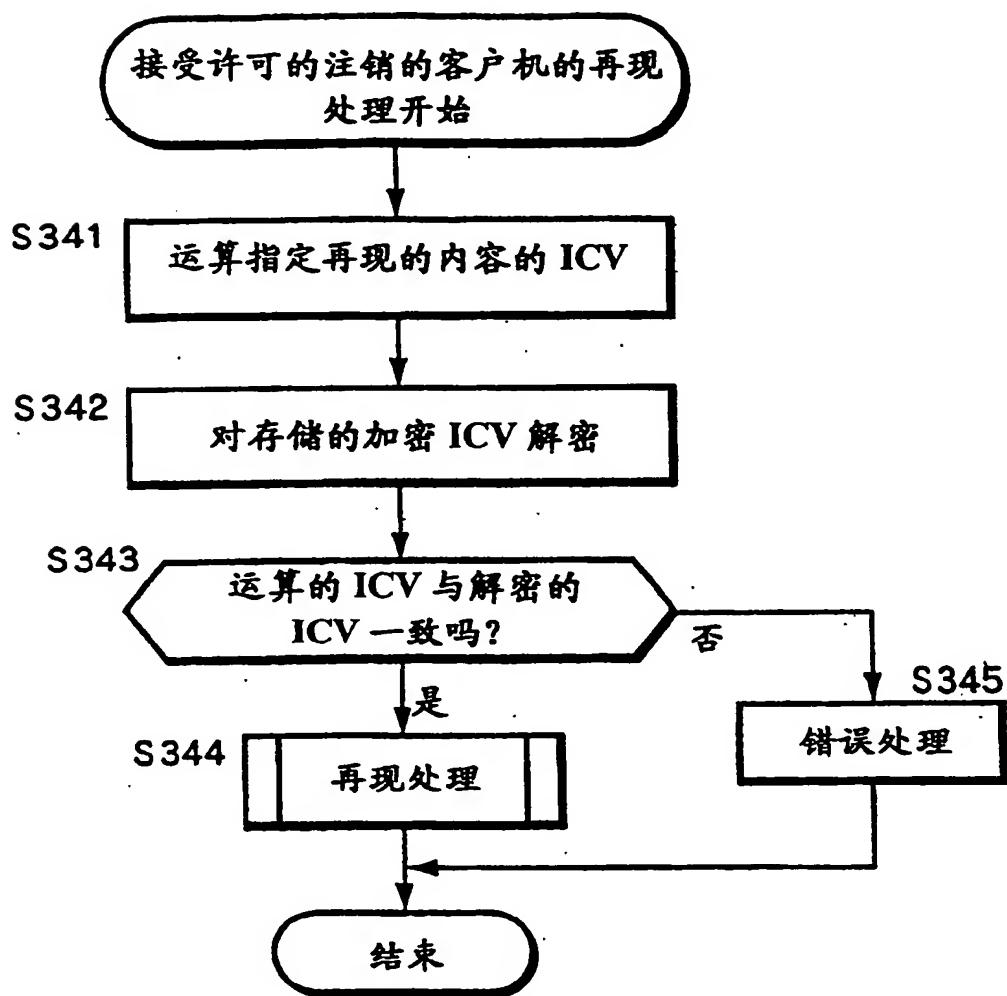


图 45

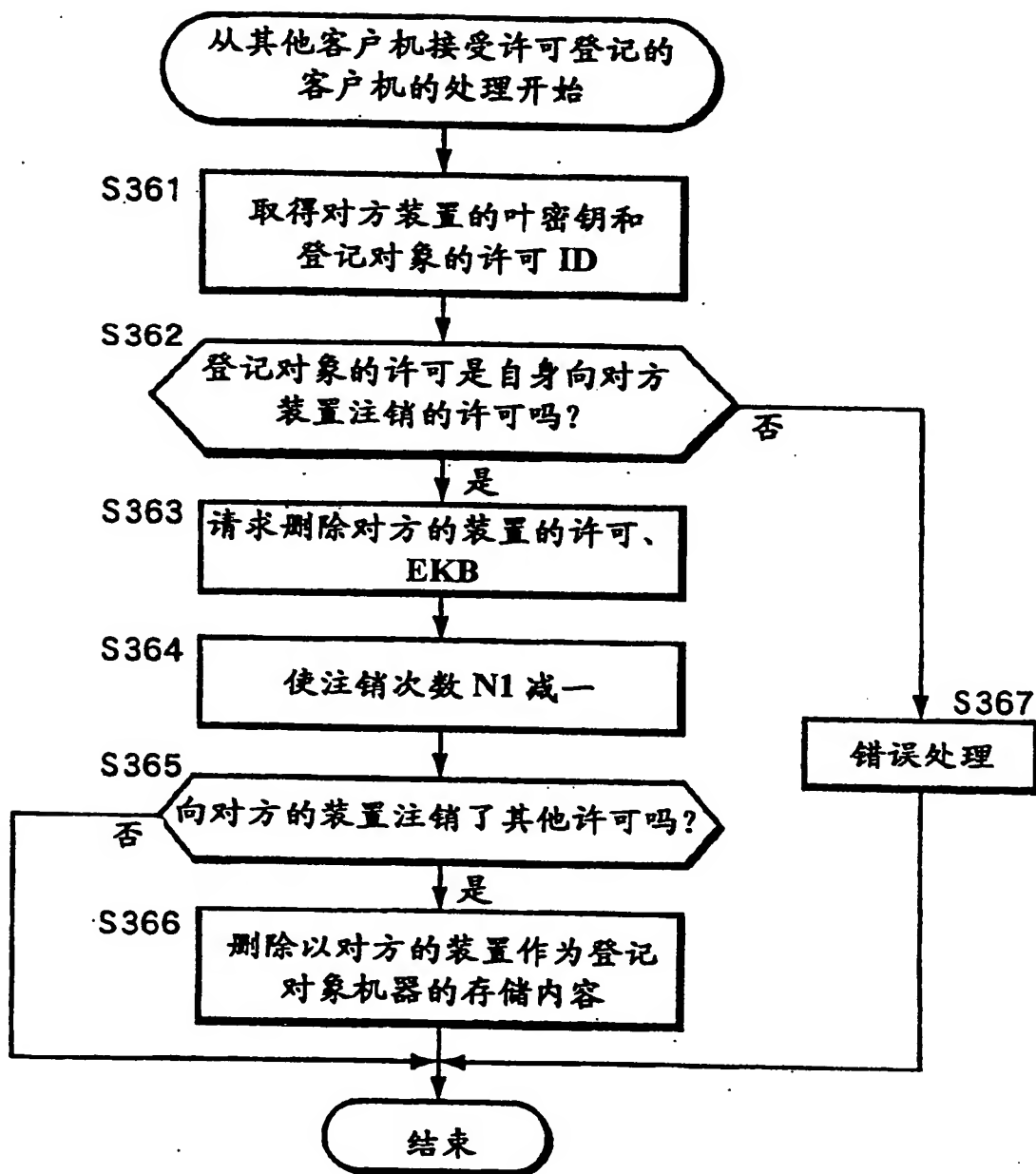


图 46

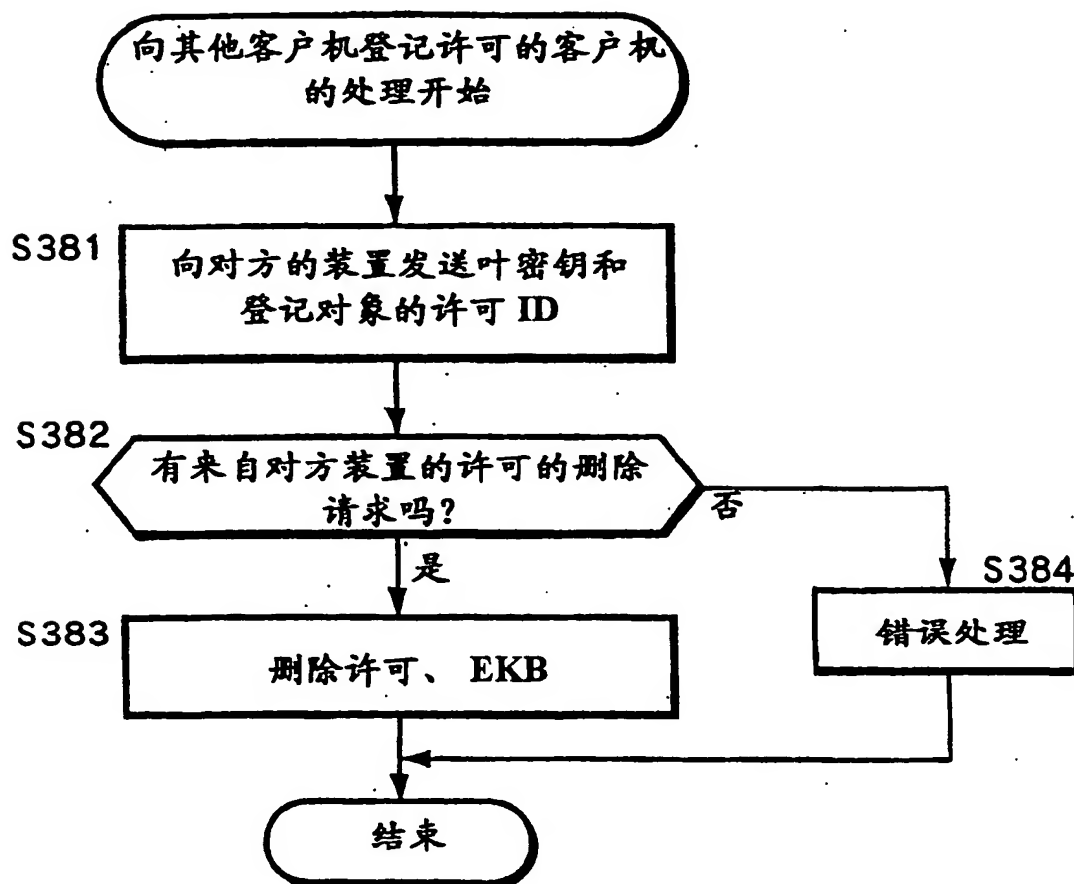


图 47

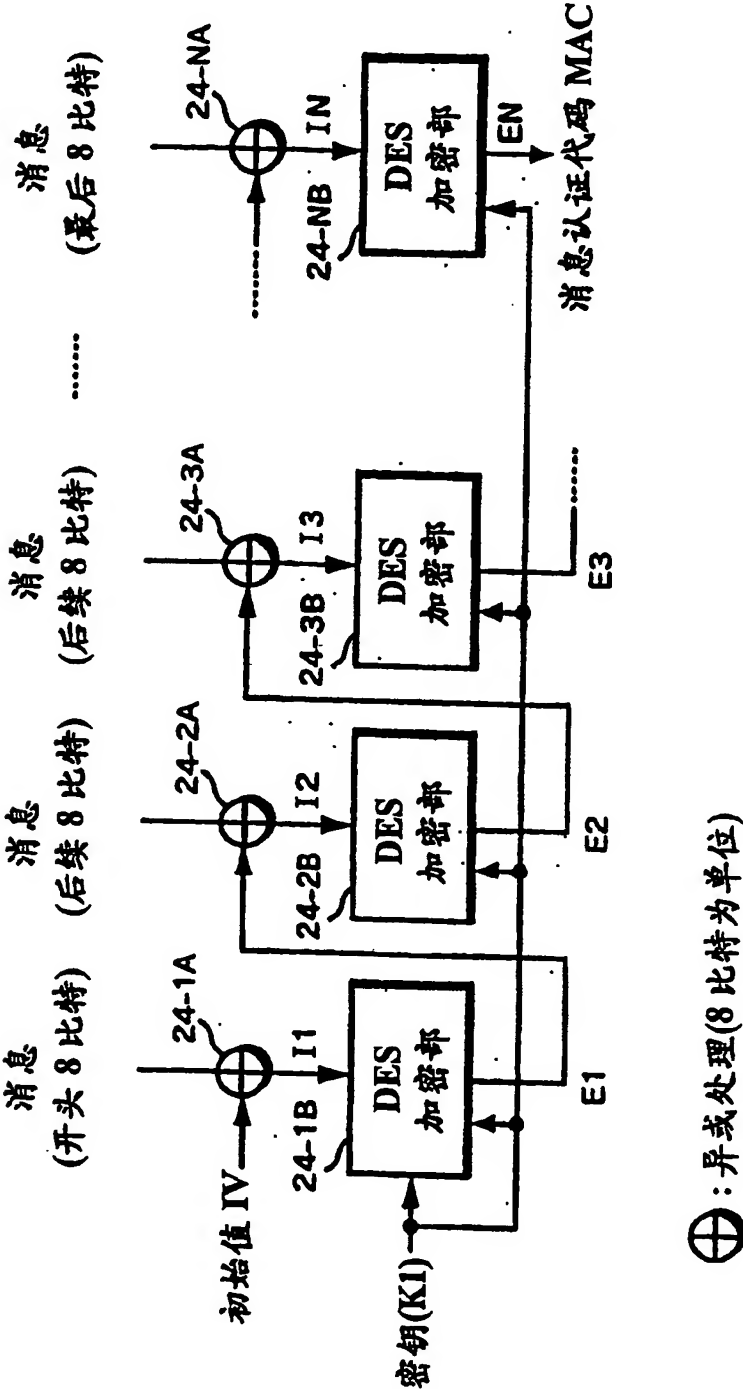
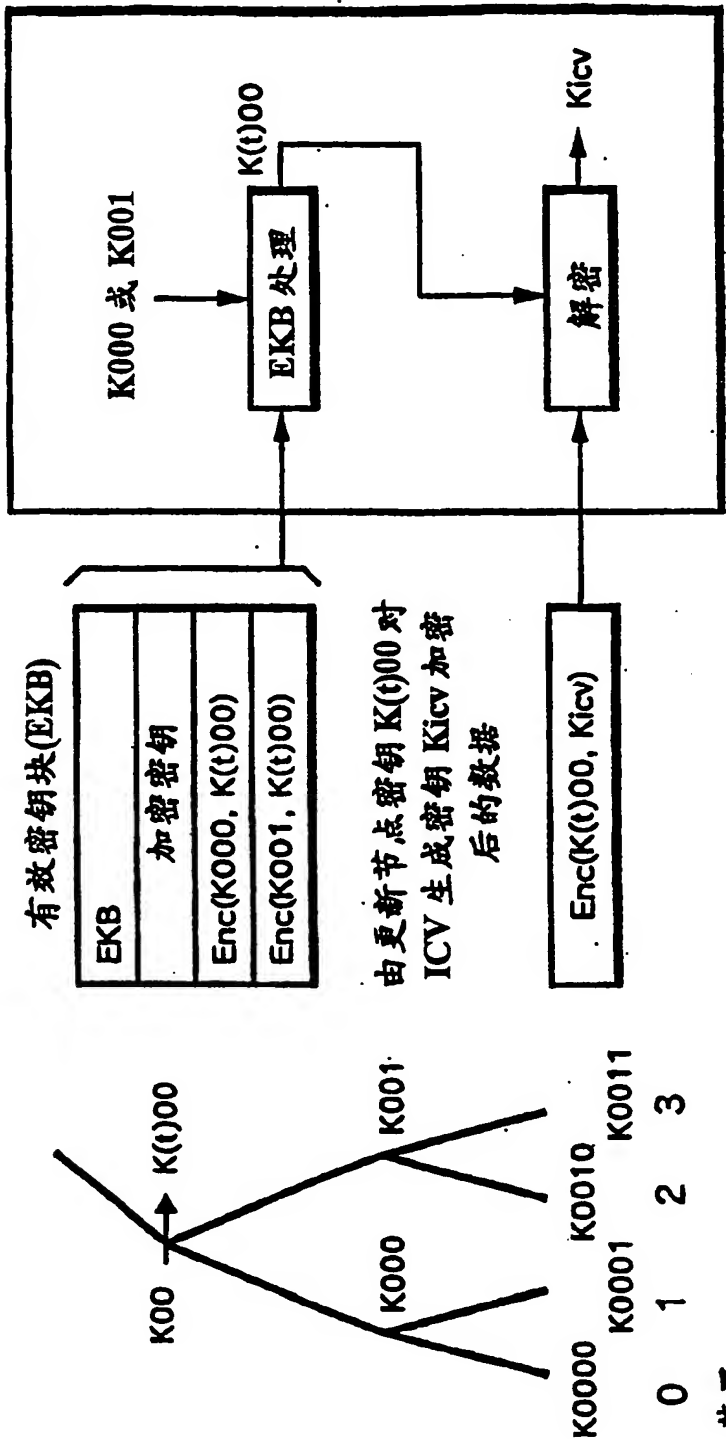
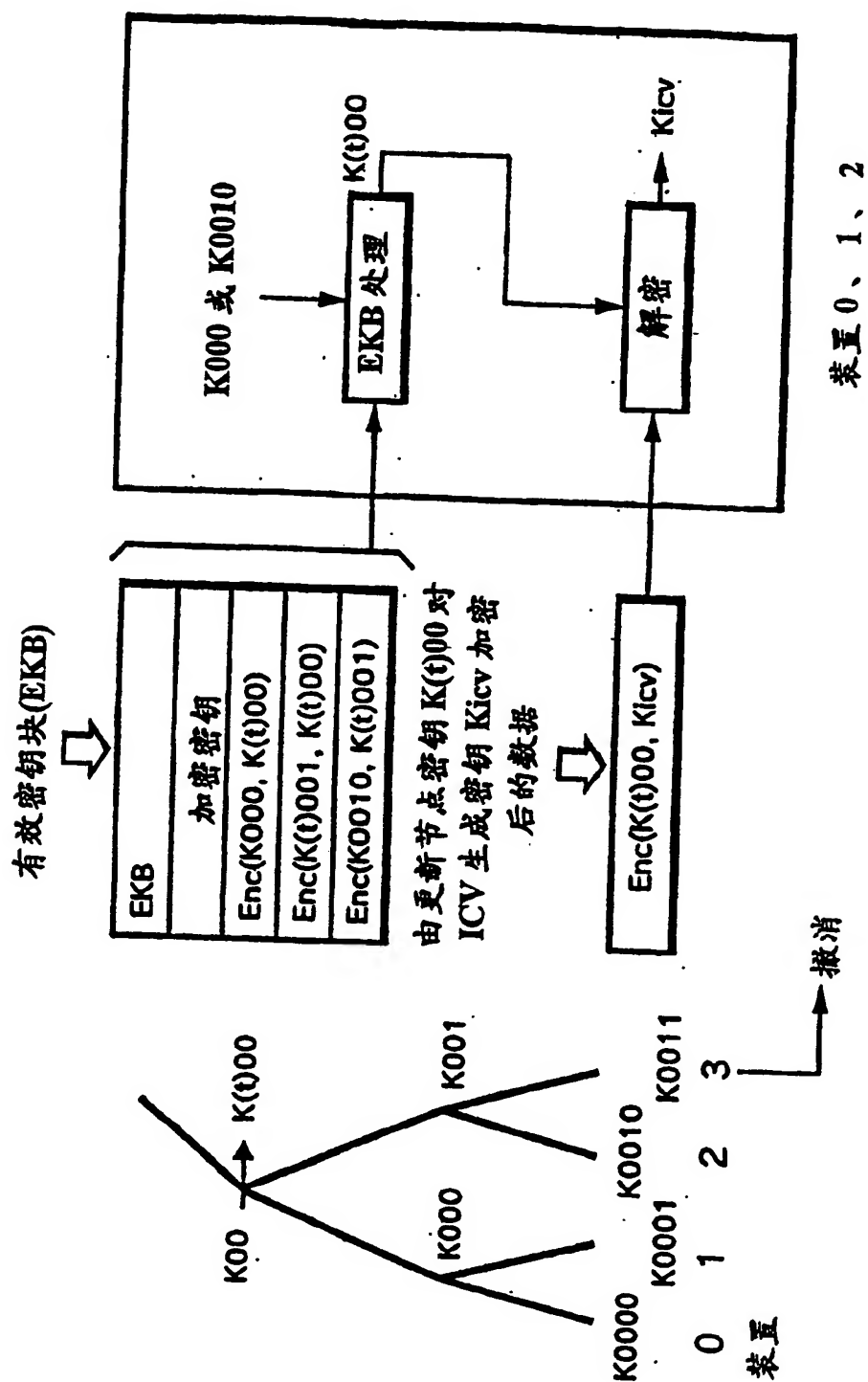


图 48



装置 0、1、2、3

图 49



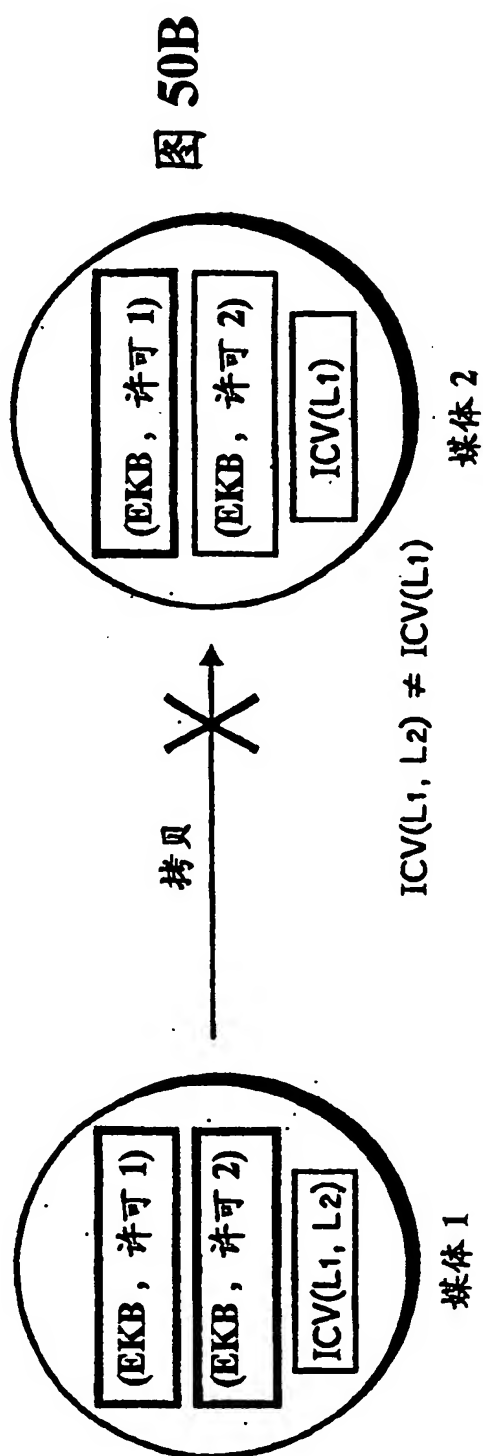
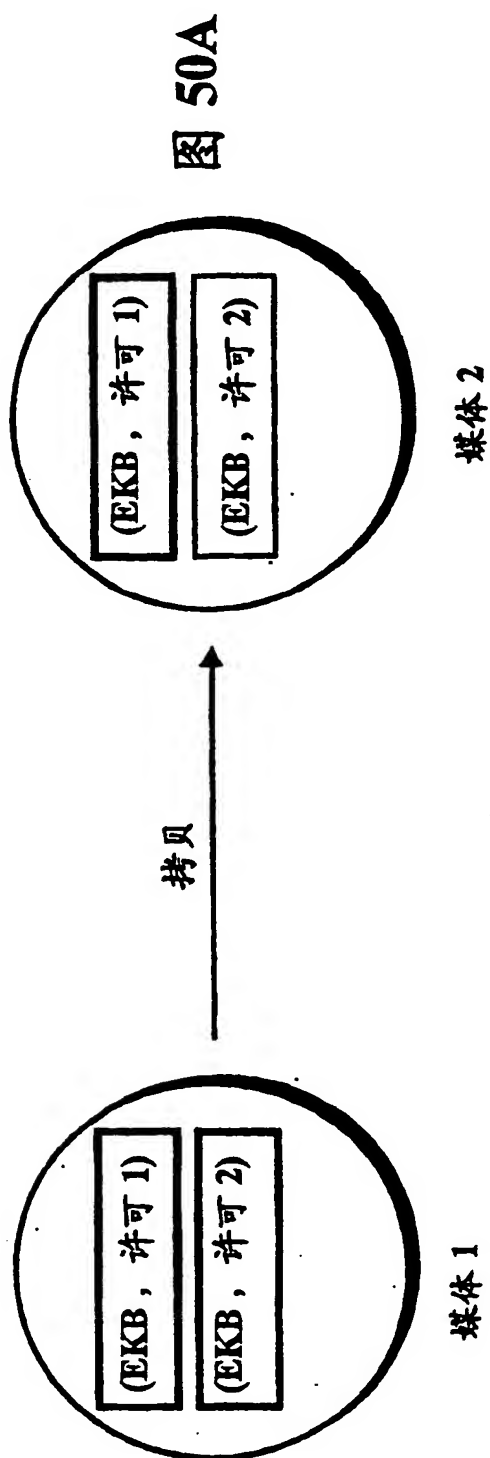
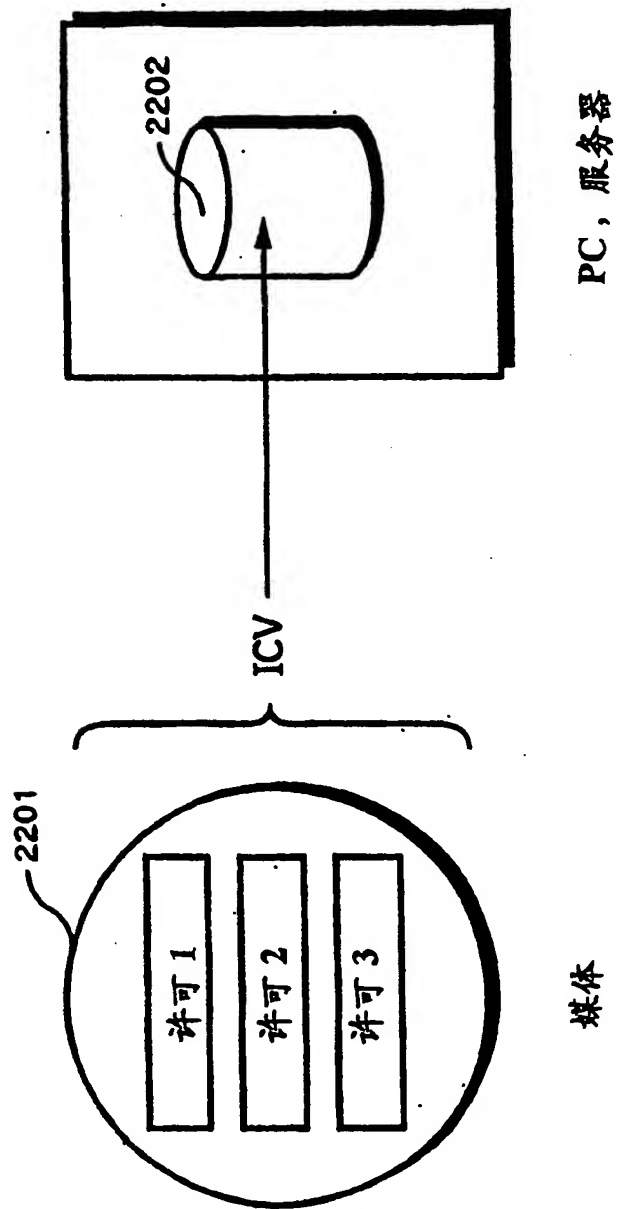


图 51



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

THIS PAGE BLACK (USPTO)